TNO-rapport
FEL-97-A003

Tokens en Biometrie voor Identificatie en Authenticatie

TNO Fysisch en Elektronisch Laboratorium

Oude Waalsdorperweg 63
Postbus 96864
2509 JG 's-Gravenhage

Telefoon 070 374 00 00
Fax 070 328 09 61

Datum
februari 1997

Auteur(s)
Ing. T.G.A. van Rhee
Ing. P.J.A. Verhaar

Rubricering

Vastgesteld door	:	LtKol P.J.G. Post Uiterweer
Vastgesteld d.d.	:	23 februari 1997
Titel	:	Ongerubriceerd
Managementuittreksel	:	Ongerubriceerd
Samenvatting	:	Ongerubriceerd
Rapporttekst	:	Ongerubriceerd
Bijlagen A - B	:	Ongerubriceerd

Exemplaarnr.	:	8	
Oplage	:	32	
Aantal pagina's	:	84	(incl. bijlagen, excl. RDP & distributielijst)
Aantal bijlagen	:	2	

TNO Fysisch en Elektronisch Laboratorium is onderdeel van de hoofdgroep TNO Defensieonderzoek waartoe verder behoren:

TNO Prins Maurits Laboratorium
TNO Technische Menskunde

Nederlandse Organisatie voor toegepast-natuurwetenschappelijk onderzoek TNO

Managementuittreksel

Titel	:	Tokens en Biometrie voor Identificatie en Authenticatie
Auteur(s)	:	Ing. T.G.A. van Rhee, Ing. P.J.A. Verhaar
Datum	:	februari 1997
Opdrachtnr.	:	A96KLu634
IWP-nr.	:	761.3
Rapportnr.	:	FEL-97-A003

De markt voor identificatie- en authenticatiemechanismen is de laatste jaren sterk in ontwikkeling. Met behulp van een identificatiemechanisme wordt de identiteit van een persoon vastgelegd en een authenticatiemechanisme dient ter controle van deze identiteit. Naast producten waarbij wachtwoorden gebruikt worden, worden producten aangeboden die gebruikmaken van tokens. Dit kunnen eenvoudige magneetkaarten zijn, maar er zijn ook ontwikkelingen waar gebruikgemaakt wordt van smart cards. Daarnaast wordt steeds vaker biometrie toegepast voor identificatie en authenticatie. Hierbij heeft biometrie betrekking op de statistiek van fysieke en gedragseigenschappen van levende individuen.

De Afdeling Militaire Inlichtingen Dienst bij de Koninklijke Luchtmacht (AMIDKLu) heeft TNO-FEL verzocht een overzicht te maken van momenteel beschikbare producten die gebruikmaken van tokens en biometrie voor de identificatie en authenticatie van personen. Dit overzicht dient ter onderbouwing van beleidskeuzes die betrekking hebben op het toepassen van dergelijke technieken binnen de Koninklijke Luchtmacht (KLu). De in het overzicht opgenomen producten dienen getoetst te worden aan een aantal dreigings-scenario's. Deze dreigingsscenario's geven reële situaties en handelingen aan die nadelige gevolgen kunnen hebben voor de KLu. De dreigingsscenario's zijn in nauwe samenwerking met de opdrachtgever opgesteld.

Dit rapport geeft aan waarom identificatie en authenticatie belangrijk is voor een organisatie. Tevens is aangegeven hoe identificatie en authenticatie kan plaatsvinden.

Daarnaast worden in dit rapport de begrippen tokens en biometrie uitgebreid beschreven om een zo goed mogelijk beeld te krijgen van de bruikbaarheid van deze begrippen bij identificatie en authenticatie. Deze beschrijvingen worden gevolgd door de beschrijvingen van de momenteel beschikbare producten, waarbij tokens en/of biometrie worden toegepast. Ook op handen zijnde ontwikkelingen op het gebied van tokens en/of biometrie zijn weergegeven.

Voor wat betreft tokens heeft het onderzoek tot de volgende conclusies geleid:

- een token dat gebruikt wordt voor identificatie of het genereren van authenticatie-informatie in een integraal onderdeel van een toegangscontrolesysteem en dient uitsluitend aan geautoriseerde personen uitgegeven te worden;
- tokens zijn gevoelig voor verlies of diefstal en dienen daarom niet gebruikt te worden als authenticatie-informatie;
- smarttokens worden voornamelijk gebruikt voor het genereren van eenmalige authenticatie-informatie.

Voor wat betreft biometrie heeft het onderzoek tot de volgende conclusies geleid:

- het gebruik van biometrische kenmerken heeft de volgende voordelen:
  - biometrische kenmerken zijn over het algemeen zeer betrouwbaar;
  - fysieke biometrische kenmerken zijn in principe onveranderlijk gedurende het leven;
  - biometrische kenmerken zijn in principe niet aan derden overdraagbaar, maar kunnen wel door derden worden ontvreemd;
  - biometrische kenmerken kunnen niet worden vergeten of verloren;
- het gebruik van biometrische kenmerken heeft de volgende nadelen:
  - biometrische kenmerken kunnen niet veranderd worden;
  - aanbieden van het biometrische kenmerk moet nauwkeurig gebeuren;
  - het gebruik van biometrische kenmerken is nog niet maatschappelijk geaccepteerd;
  - de bezitter van een kenmerk loopt grote risico's, wanneer derden dit kenmerk proberen te ontvreemden;
- de betrouwbaarheid van een systeem dat gebruikmaakt van biometrische kenmerken wordt aangegeven met de 'False Acceptance Rate' (FAR) en de 'False Rejection Rate' (FRR). Een hoge FAR geeft een minder betrouwbare methode, maar heeft een hoge gebruikersacceptatie. Een hoge FRR geeft een betrouwbare methode, maar heeft een lage gebruikersacceptatie tot gevolg;
- de integriteit van de gebruikersrepresentatie is van groot belang;
- de gebruikersacceptatie is afhankelijk van:
  - gebruiksgemak;
  - risico's voor de bezitters van het kenmerk.

Naast de conclusies met betrekking tot tokens en biometrie zijn tijdens het onderzoek de volgende conclusies ontstaan:

- de binnen het onderzoek onderkende beveiligingsgebieden van diverse gradaties zijn af te dekken door het gebruik van tokens in combinatie met wachtwoorden of biometrische kenmerken;
- de biometrische kenmerken retrinapatroon en irispatroon zijn momenteel het betrouwbaarst. Echter de gebruikersacceptatie is minimaal;
- de kenmerken vingerafdruk, statische en dynamische handtekening zijn relatief eenvoudig te vervalsen, maar hebben een hoge gebruikersacceptatie;
- de kenmerken handgeometrie en vingergeometrie zijn aanzienlijk moeilijker te vervalsen als de vingerafdruk. De gebruikersacceptantie is goed te noemen.

Tot slot worden de volgende aanbevelingen gedaan:

- om het vertrouwen in het toegangscontrolesysteem te vergroten, wordt aanbevolen smarttokens te gebruiken voor het genereren van eenmalig te gebruiken authenticatie-informatie;
- dezelfde aanbeveling geldt, wanneer geautoriseerde personen communiceren met een organisatie die niet wordt vertrouwd;
- om de gevolgen van de dreigingen verlies en diefstal te verminderen wordt aanbevolen dumbtokens uitsluitend te gebruiken voor identificatie, gecombineerd met authenticatie door middel van wachtwoorden of biometrie;
- aanbevolen wordt de producten in de praktijk te onderzoeken en te testen. Tijdens het testen van producten dient ook gekeken te worden naar de diverse combinatiemogelijkheden van tokens en biometrische kenmerken.

Samenvatting

De laatste jaren is er veel voortuitgang geboekt in de ontwikkeling van identificatie- en authenticatiemechanismen. Zo worden steeds vaker tokens toegepast. Dit kunnen eenvoudige magneetkaarten zijn, maar er zijn ook ontwikkelingen waar gebruikgemaakt wordt van (super)smart cards. Deze (super)smart cards kunnen geheel zelfstandig berekeningen uitvoeren. Ook worden steeds vaker biometrische eigenschappen van een persoon toegepast voor identificatie en authenticatie. Om een inzicht te krijgen in de momenteel beschikbare producten en ontwikkelingen heeft TNO-FEL de opdracht gekregen van de Afdeling Militaire Inlichtingen Dienst bij de Koninklijke Luchtmacht (AMIDKLu) een overzicht te maken.

De in het overzicht opgenomen producten worden tevens getoetst aan een aantal geselecteerde dreigingsscenario's. Deze dreigingsscenario's zijn in overleg met de opdrachtgever opgesteld. Deze toetsing wordt verricht ter onderbouwing van eventuele beleidskeuzes met betrekking tot het toepassen van dergelijke producten.

Inhoud

1. Inleiding

De markt voor identificatie- en authenticatiemechanismen is de laatste jaren sterk in ontwikkeling. Met behulp van een identificatiemechanisme wordt de identiteit van een persoon vastgelegd en een authenticatiemechanisme dient ter controle van deze identiteit. Naast de conventionele producten waarbij wachtwoorden gebruikt worden, worden producten aangeboden die gebruikmaken van tokens. Deze tokens kunnen eenvoudige magneetkaarten zijn, maar er zijn ook producten die gebruikmaken van (super)smart cards die geheel zelfstandig berekeningen kunnen uitvoeren. Daarnaast wordt steeds vaker biometrie toegepast voor identificatie en authenticatie. Hierbij heeft biometrie betrekking op de statistiek van fysieke en gedragseigenschappen van levende individuen.

De Afdeling Militaire Inlichtingen Dienst bij de Koninklijke Luchtmacht (AMIDKLu) heeft TNO-FEL verzocht een overzicht op te stellen, ten behoeve van de Koninklijke Luchtmacht (KLu), van de op dit moment beschikbare producten, waarbij identificatie en authenticatie plaatsvindt met behulp van tokens of biometrische eigenschappen. Dit overzicht dient ter onderbouwing van eventuele beleidskeuzes met betrekking tot het toepassen van deze technieken binnen de KLu. Ook zal aandacht worden besteed aan de tendensen in de ontwikkeling van producten op dit gebied.

Tevens worden de in het overzicht opgenomen producten getoetst aan een lijst van dreigingsscenario's. Deze dreigingsscenario's zijn in overleg met de opdrachtgever opgesteld.

1.1 Afbakening

Het onderzoek zal worden uitgevoerd aan de hand van de huidige (commerciële) markt van producten voor identificatie en authenticatie met behulp van tokens of biometrische eigenschappen.

Met name op het gebied van biometrische eigenschappen zijn de betrouwbaarheid en de acceptatie door de gebruiker belangrijke parameters voor de toepasbaarheid. Deze parameters worden zo goed als mogelijk in kaart gebracht.

De verkregen productgegevens zullen worden toegevoegd aan de database met informatiebeveiligingsproducten (MITBEP).

1.2 Indeling van het rapport

In hoofdstuk 2 wordt een korte beschrijving gegevens van de begrippen identificatie en authenticatie.

In hoofdstuk 3 wordt aangegeven hoe identificatie en authenticatie kan worden gerealiseerd met behulp van tokens. Hiertoe wordt in eerste instantie een beschrijving gegeven van de mogelijkheden en uitvoeringsvormen van tokens. Daarnaast wordt in dit hoofdstuk aangegeven welke producten momenteel verkrijgbaar zijn en welke ontwikkelingen gaande zijn.

In het volgende hoofdstuk wordt aangegeven hoe identificatie en authenticatie kan worden gerealiseerd met behulp van biometrische eigenschappen. Ook in dit hoofdstuk wordt eerst een beschrijving gegeven van de mogelijkheden van biometrische eigenschappen. Daarnaast wordt ook aangegeven welke producten momenteel verkrijgbaar zijn en welke ontwikkelingen gaande zijn.

In hoofdstuk 5 wordt beschreven welke mogelijkheden er zijn voor producten die tokens en biometrische eigenschappen combineren, om te komen tot identificatie en authenticatie.

In hoofdstuk 6 worden relevante dreigingsscenario's beschreven, die in hoofdstuk 7 worden gebruikt om de beschreven producten te toetsen.

Tot slot worden in hoofdstuk 8 conclusies en aanbevelingen opgesomd.

2. Identificatie en authenticatie

Binnen een organisatie bevindt zich informatie die van belang is voor het goed functioneren van de bedrijfsprocessen van deze organisatie. Deze informatie kan op verschillende manieren zijn opgeslagen, bijvoorbeeld in de vorm van papieren documenten. Echter een steeds grotere hoeveelheid informatie zal, in elektronische vorm, zijn opgeslagen in informatiesystemen. Bescherming van een deel van deze informatie is belangrijk voor de organisatie, omdat:

- de voortgang van de bedrijfsprocessen afhankelijk kan zijn van de aanwezigheid van deze informatie (beschikbaarheid);
- de voortgang van de bedrijfsprocessen afhankelijk kan zijn van de juistheid, actualiteit en de volledigheid van deze informatie (integriteit);
- toegang tot of kennisname van informatie door 'concurrerende' organisaties nadelige gevolgen kan hebben voor de organisatie (exclusiviteit).

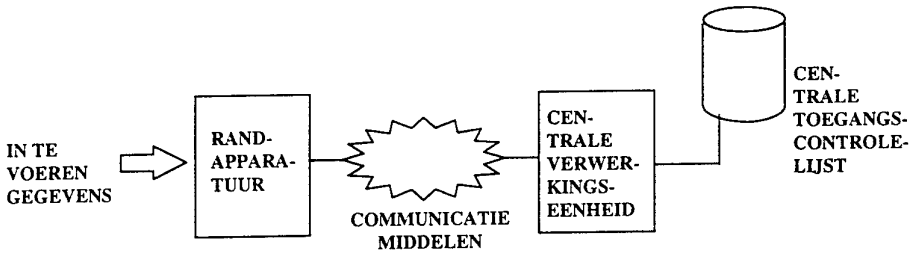
Uit oogpunt van beheer en beveiliging is het gewenst de toegang tot de waardevolle informatie te controleren. De eerste stap tot het beheren en beveiligen van deze informatie is de toegang te controleren tot locaties en/of informatiesystemen, waar de waardevolle informatie is opgeslagen. Dit proces wordt ook wel toegangscontrole genoemd. De controle kan plaatsvinden elke keer dat een persoon een locatie opnieuw wil betreden of elke keer dat deze persoon toegang wenst tot een informatiesysteem. Op deze manier worden dan alleen geautoriseerde personen toegelaten. Tevens kan de aanwezigheid van de persoon incidenteel, periodiek of continu gecontroleerd worden.

Tijdens de toegangscontrole vindt er een uitwisseling van gegevens plaats tussen de persoon die toegang wenst en het toegangscontrolesysteem. Dit toegangscontrolesysteem bepaalt aan de hand van de uitgewisselde gegevens of de persoon in kwestie recht heeft op toegang tot de betreffende locatie en/of het informatiesysteem. Hiertoe is in het toegangscontrolesysteem een toegangscontrolelijst opgeslagen. Deze toegangscontrolelijst bevat een aantal specifieke gegevens van de geautoriseerde personen.

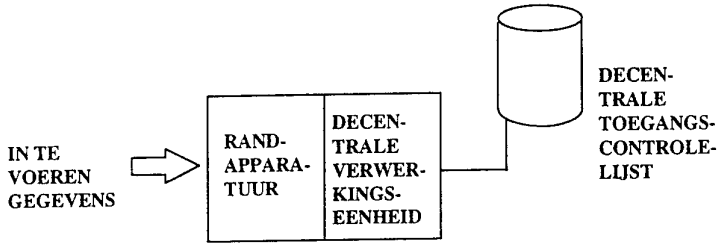
Wanneer het toegangscontrolesysteem is geautomatiseerd, kan het bestaan uit:

- centrale of decentrale verwerkingseenheden, in de vorm van computersystemen;
- randapparatuur voor de invoering van de te controleren gegevens;
- communicatiemiddelen tussen randapparatuur en verwerkingseenheden;
- een database waarin de toegangscontrolelijst is opgenomen.

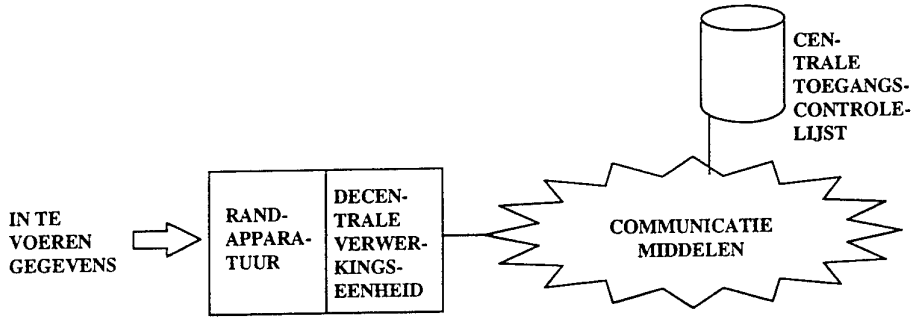
In de figuren 2.1 t/m 2.3 zijn de mogelijke architecturen weergegeven van een toegangscontrolesysteem.



Figuur 2.1: Toegangscontrolesysteem waarbij de verwerking van ingevoerde gegevens centraal plaatsvindt. Ook de toegangscontrolelijst is bij dit systeem centraal opgeslagen.



Figuur 2.2: Toegangscontrolessyteem waarbij de verwerking van de ingevoerde gegevens decentraal plaatsvindt. Ook de toegangscontrolelijst is bij dit systeem decentraal opgeslagen.



Figuur 2.3: Toegangscontrolesysteem waarbij de verwerking van de ingevoerde gegevens decentraal plaatsvindt. De toegangscontrolelijst is hier echter centraal opgeslagen.

2.1 Identificatie

Een toegangscontrole kan worden uitgevoerd door autorisatie te verlenen aan personen die, uit hoofde van hun functie, toegang dienen te krijgen tot de informatie. De verkregen autorisatie wordt gekoppeld aan de 'identiteit' van de betreffende personen en wordt opgenomen in een toegangslijst. Deze identiteit is over het algemeen een representatie van de werkelijke identiteit van een persoon. Met andere woorden: de identiteit is een gegeven waaronder een persoon **bekend** is binnen een toegangscontrolesysteem van een locatie en/of informatiesysteem.

Deze identiteit dient uniek te zijn, zodat het toegangscontrolesysteem éénduidig kan vastleggen welke persoon verbonden is aan deze identiteit.

Wanneer een van deze personen toegang wil tot de informatie dient zijn of haar identiteit kenbaar gemaakt te worden. Met behulp van deze identiteit kan dan bepaald worden of de betrokken persoon voorkomt op een toegangslijst en welke rechten deze persoon heeft. Het kenbaar maken van de identiteit door de betrokken persoon gevolgd door het vaststellen van de identiteit door het toegangscontrolesysteem wordt ook wel identificatie genoemd. Bij identificatie wordt slechts gecontroleerd of de identiteit van de betreffende persoon voorkomt op een zogenaamde toegangslijst. Er wordt niet gecontroleerd of de betreffende persoon is wie hij beweert te zijn.

Identificatie kan plaatsvinden aan de hand van:
- iets wat een persoon **bezit** (zoals een sleutel of een token);
- iets wat een persoon **weet** (zoals een user-id), of;
- iets wat een persoon **is** (zoals biometrische eigenschappen).

Het verlenen van toegang, tot een locatie en/of informatiesysteem, op basis van uitsluitend identificatie kan de nodige risico's opleveren. In een dergelijke situatie dient de in de toegangslijst opgenomen identiteit alleen reproduceerbaar te zijn door de betrokken, geautoriseerde persoon. Is de identiteit van de geautoriseerde persoon toch reproduceerbaar door ongeautoriseerde personen, dan kunnen deze ongeautoriseerde personen alsnog toegang verkrijgen tot een locatie en/of informatiesysteem door een 'valse' identiteit te claimen.

In tegenstelling tot de andere mogelijkheden is 'iets wat een persoon bezit' bij verlies of diefstal door derden te gebruiken om toegang te krijgen tot de betreffende locatie en/of informatiesysteem. Hierdoor kan identificatie op basis van 'iets wat een persoon bezit' als de zwakste van de 3 mogelijkheden worden beschouwd. Wanneer dit 'iets wat een persoon bezit' wordt verloren of ontvreemd, heeft:
- de persoon in kwestie geen toegang meer tot de betreffende locatie en/of informatiesysteem;
- een ongeautoriseerd persoon de mogelijkheid zonder problemen toegang te verkrijgen tot de betreffende locatie en/of informatiesysteem.

Voor 'iets wat een persoon weet' geldt: wanneer de geautoriseerde persoon dit gegeven niet meer kan reproduceren krijgt hij geen toegang meer tot de betreffende locatie en/of informatiesysteem. Een ongeautoriseerde persoon krijgt in principe geen toegang, wanneer de geautoriseerde persoon zijn identiteit 'kwijt' is. Wel dient opgemerkt te worden dat 'iets wat een persoon weet' niet makkelijk te raden moet zijn voor ongeautoriseerde personen. Enkele voorbeelden hiervan zijn:
- geen namen van familieleden, vrienden, partners, huisdieren, enz. voor wachtwoorden;

- geen (makkelijke) bestaande woorden of eenvoudige combinaties van letters voor wachtwoorden;
- geen makkelijke combinaties voor PIN-codes.

Voor 'iets wat een persoon is' geldt dat alle (biometrische) eigenschappen, die als identiteit gebruikt kunnen worden, in principe niet aan derden overdraagbaar zijn. Biometrische eigenschappen hebben het volgende grote voordeel. Al is een ongeautoriseerd persoon op de hoogte van een biometrische eigenschap van een geautoriseerde persoon, de eigenschap is niet of nauwelijks reproduceerbaar. De persoon hoeft zijn identiteit ook niet te onthouden of mee te nemen, omdat de identiteit altijd beschikbaar is.

Er dient opgemerkt te worden dat voor de drie identificatiemogelijkheden geldt dat het voor een ongeautoriseerd persoon altijd mogelijk is de identiteit van een geautoriseerd persoon onder dwang te bemachtigen.

2.2 Authenticatie (of verificatie van de identiteit)

Om meer vertrouwen te krijgen in de identiteit van een persoon (is de persoon wie hij beweert te zijn?), dient de kenbaar gemaakte identiteit geverifieerd te worden. De vastgestelde identiteit dient gekoppeld te kunnen worden aan de persoon die de identiteit aangeboden heeft. Dit verifiëren vindt plaats door één of meer gegevens te koppelen aan de identiteit van één persoon. In dit geval hoeft de identiteit van de betrokken persoon niet noodzakelijkerwijs geheim te zijn. Wel dienen de gegevens die de verificatie mogelijk maken niet of nauwelijks reproduceerbaar te zijn door derden, of geheim te zijn. Het proces dat de kenbaar gemaakte identiteit verifieert wordt ook wel authenticatie genoemd. De, aan de identiteit van één persoon, te koppelen gegevens worden aangeduid als authenticatie-informatie. Door authenticatie ontstaat meer zekerheid/vertrouwen in de identiteit van een persoon. De waarschijnlijkheid dat de kenbaar gemaakte identiteit overeenkomt met de werkelijke identiteit wordt groter.

Authenticatie kan plaatsvinden door twee of meer van de mogelijkheden om te komen tot identificatie (iets wat een persoon bezit, weet en is) te combineren. Eén van de mogelijkheden wordt gebruikt voor de identificatie van de persoon. De rest wordt gebruikt voor de authenticatie van deze persoon. Zoals al in de voorgaande alinea is aangegeven dienen de gegevens die gebruikt worden voor de authenticatie niet of nauwelijks reproduceerbaar te zijn door derden, of geheim te zijn. Enkele voorbeelden hiervan zijn:

- een klantnummer voor de identificatie (iets wat een persoon weet) in combinatie met een PIN-code voor de authenticatie (iets wat alleen de juiste persoon weet);

- een token dat gebruikt wordt voor de identificatie (iets wat een persoon bezit) in combinatie met een PIN-code of wachtwoord voor de authenticatie (iets wat alleen de juiste persoon weet);
- een token dat gebruikt wordt voor de identificatie (iets wat een persoon bezit) in combinatie met een biometrische eigenschap voor de authenticatie (iets wat alleen de juiste persoon is);
- een biometrische eigenschap voor de identificatie (iets wat de persoon is) in combinatie met een wachtwoord of PIN-code voor authenticatie (iets wat alleen de juiste persoon weet);
- een token dat gebruikt wordt voor de identificatie (iets wat een persoon bezit) in combinatie met een PIN-code of wachtwoord (iets wat alleen de juiste persoon weet) en een biometrische eigenschap voor de authenticatie (iets wat alleen de juiste persoon is).

In de hoofdstukken 'Identificatie en authenticatie met behulp van tokens' en 'Identificatie en authenticatie met behulp van biometrische kenmerken' zal verder ingegaan worden op specifieke technieken die voor identificatie en authenticatie gebruikt kunnen worden.

3. Identificatie en authenticatie met behulp van tokens

Identificatie en authenticatie met behulp van tokens is gebaseerd op 'iets wat een persoon bezit'. Hierbij dient de gebruiker een token te kunnen tonen aan het toegangscontrolesysteem, dat op zijn beurt het token kan herkennen als 'horende bij een legitieme gebruiker'. Het token wordt over het algemeen gebruikt voor de identificatie van de gebruiker. Voor de authenticatie kan gebruikgemaakt worden van 'iets wat een persoon weet' en 'iets wat een persoon is'. Door de steeds verdergaande ontwikkelingen kunnen tokens ook gebruikt worden voor het genereren van 'iets wat een persoon weet'. Hiervoor wordt gebruikgemaakt van zogenaamde smarttokens, zoals chipcards op PC-cards. In principe worden de tokens dan nog steeds gebruikt voor identificatie. In paragraaf 3.1 zal verder ingegaan worden op tokens in het algemeen.

Bij het gebruik van smarttokens, voor het genereren van 'iets wat een persoon weet', is het voor de gebruiker vaak toch nog nodig een wachtwoord of PIN-code te gebruiken om het smarttoken te activeren. In paragraaf 3.2 zal verder ingegaan worden op mogelijke technieken, voor identificatie en authenticatie, die gebruikmaken van tokens.

Tot slot zal in paragraaf 3.3 een overzicht worden gegeven van bestaande producten en ontwikkelingen op het gebied van identificatie en authenticatie met behulp van tokens.

3.1 Tokens

Een token is in principe een fysiek medium waarop informatie kan worden opgeslagen. Tokens worden voornamelijk toegepast:

- als opslagmedium voor:
  - data;
  - cryptografisch materiaal;
- voor identificatie van personen, dieren en/of producten;
- voor het genereren van authenticatie-informatie.

Het onderzoek zal zich verder toespitsen op tokens voor identificatie van personen en tokens die gebruikt worden voor het genereren van authenticatie-informatie. De overige tokens vallen buiten de doelstelling van dit onderzoek. Wel zullen, in deze paragraaf, voor de completering van een opsomming van mogelijke tokens, voorbeelden van deze tokens worden gegeven.

Tokens die gebruikt worden voor identificatie en authenticatie vertegenwoordigen een deel van het toegangscontrolesysteem. Wanneer het toegangscontrolesysteem is geautomatiseerd kan het verder bestaan uit:

- centrale of decentrale verwerkingseenheden, in de vorm van computersystemen;
- randapparatuur voor de communicatie tussen de tokens en de verwerkingseenheden;
- communicatiemiddelen tussen randapparatuur en verwerkingseenheden.

De tokens zijn in het bezit van de personen die zijn opgenomen in de toegangscontrolelijst. Door het aanbieden van de tokens aan de randapparatuur wordt het toegangscontroleproces opgestart.

3.1.1 Mogelijke technische onderverdelingen bij tokens

Tokens kunnen worden ingedeeld naar de manier waarop gegevens op of in het token worden opgeslagen. Met tokens kunnen gegevens fysiek, magnetisch, optisch en/of elektronisch opgeslagen worden.

Tevens kunnen tokens worden ingedeeld naar de intelligentie die ze bezitten. Er zijn tokens die uitsluitend over opslagcapaciteit beschikken. Deze tokens worden ook wel dumbtokens genoemd. Daarnaast zijn er tokens die beschikken over de mogelijkheid om bewerkingen uit te kunnen voeren. Naast opslagcapaciteit bevatten deze tokens een processor die deze bewerkingen kan uitvoeren. Dergelijke tokens worden ook wel smarttokens genoemd.

Daarnaast is onderscheid te maken tussen tokens die wel of niet over een eigen voedingsbron beschikken. Voor tokens die gebruikmaken van 'vluchtige' geheugens zijn eigen voedingsbronnen noodzakelijk, wanneer de opgeslagen gegevens behouden dienen te worden. Smarttokens met een eigen voedingsbron kunnen zelfstandig hun bewerkingen uitvoeren. Smarttokens zonder eigen voedingsbron zijn afhankelijk van externe voedingsbronnen. Deze externe voedingsbronnen worden voornamelijk aangeboden door de randapparatuur van de geautomatiseerde toegangscontrolesystemen, waarmee de tokens communiceren.

Ook zijn er tokens die beschikken over een eigen interface naar de gebruiker toe. Het token kan dan bijvoorbeeld beschikken over een display, waarop informatie kan worden uitgelezen. Ook kan het token beschikken over een toetsenbord (bijvoorbeeld een keyboard of PIN-pad), waarmee informatie kan worden ingevoerd in het token. Dergelijke tokens worden ook wel supertokens genoemd.

Als laatste wordt onderscheid gemaakt in de manier waarop tokens communiceren met geautomatiseerde toegangscontrolesystemen. De volgende mogelijkheden worden onderkend:

- tokens kunnen communiceren met de randapparatuur door middel van het maken van (elektronische) contacten (contactcommunicatie);
- tokens kunnen communiceren met de randapparatuur door middel van Radio Frequenties (RF-communicatie of contactloze communicatie).

3.1.2 Voor- en nadelen tokens

Het voordeel van het gebruik van tokens voor identificatie en authenticatie is dat het token wordt uitgegeven aan geautoriseerde personen. Hierdoor zijn in principe de betrokken personen bekend.

Het nadeel is dat tokens kunnen worden verloren, gestolen, nagemaakt of uitgelezen.

Het is mogelijk dat de authenticatie-informatie wordt uitgelezen door onbevoegden. Een dergelijke dreiging kan ontstaan wanneer randapparatuur van het toegangscontrolesysteem buiten de gecontroleerde omgeving van de organisatie staat opgesteld. Tevens kan deze dreiging optreden als de organisatie waarmee gecommuniceerd wordt niet voldoende kan worden vertrouwd. Personeel van de organisatie zou gegevens kunnen uitlezen van randapparatuur of communicatiekanalen. Het achterhalen van authenticatie-informatie wordt zinloos wanneer ieder authenticatieproces voor iedere sessie andere authenticatie-informatie genereert.

Doordat smarttokens zelf bewerkingen kunnen uitvoeren en dus bij iedere sessie nieuwe authenticatie-informatie kunnen aanmaken, kunnen deze tokens worden toegepast wanneer:

- de organisatie waarmee gecommuniceerd wordt niet kan worden vertrouwd, of;
- de randapparatuur waarmee wordt gecommuniceerd niet kan worden vertrouwd.

3.1.3 Mogelijke uitvoeringsvormen van tokens

Een token is in principe niet gebonden aan bepaalde afmetingen. Wel zijn er tokens waarvan de afmetingen zijn gestandaardiseerd. Hieronder vallen o.a. alle tokens die de afmetingen van een creditcard hebben. Een voorbeeld van een dergelijk token is een chipcard. Een opsomming van verschillende uitvoeringsvormen van tokens volgt in een zo volledig mogelijk overzicht. Opgemerkt dient te worden dat uitgegaan is van fysieke vormen. Hierbij is het bijvoorbeeld niet uit te sluiten dat een token met de fysieke vorm van een sleutel, qua functionaliteit, wordt gerangschikt onder de categorie labels.

Sleutels

Hiermee worden bedoeld: fysieke sleutels, waarbij het bezit van deze sleutels, toegang biedt tot een locatie, een ruimte en/of een informatiesysteem. Dergelijke tokens zijn zowel zonder geheugen en/of intelligentie als met geheugen en/of intelligentie uit te voeren. Zijn de sleutels uitgevoerd met geheugen en/of intelligentie dan is het mogelijk de gebruiker van de sleutel te authenticeren.

Dongles

Een dongle is een stukje hardware dat wordt aangeboden op een poort van een (personal) computersysteem. Bepaalde softwarepakketten maken gebruik van een dongle om zodoende het kopiëren van deze software tegen te gaan. Wanneer bij

het opstarten van dit softwarepakket, of tijdens het gebruik, het dongle niet aanwezig is wordt (een deel van) de functionaliteit van dit softwarepakket niet geactiveerd.

Labels

Een label is een token dat informatie bevat. De afmetingen van labels zijn niet of nauwelijks gestandaardiseerd. Een label kenmerkt zich doordat de informatie op afstand is uit te lezen. De communicatieprotocollen van labels zijn niet of nauwelijks gestandaardiseerd. Afhankelijk van de manier waarop deze informatie is opgeslagen kan het uitlezen plaatsvinden door middel van:

- optisch uitlezen (bij het uitlezen van opdruk);
- uitlezen met behulp van Radio Frequenties (RF) (bij het uitlezen van elektronisch opgeslagen informatie);
- uitlezen met behulp van elektromagnetische velden (bij het uitlezen van magnetisch opgeslagen informatie).

Deze tokens worden veelvuldig gebruikt voor het bepalen van het gedragspatroon of de transportweg van dieren en producten. Daarbij is de identificatie van deze dieren of producten van groot belang.

Kaarten

Ook dit zijn tokens die informatie bevatten. Het verschil met labels zit in de vorm van het token. De naam maakt duidelijk dat het token de vorm van een kaart dient te hebben. Ook zijn niet alle kaarten op afstand uit te lezen.

In tegenstelling tot labels is een groot deel van de kaarten wel gestandaardiseerd voor wat betreft de afmetingen. Deze afmetingen zijn conform ISO standaarden [1] (het zogenaamde creditcard formaat).

De volgende verschijningsvormen zijn te onderkennen:

- bedrukte kaarten (zogenaamde badges);
- embossed card: De embossed-kaart is een kunststof kaartje waarbij gegevens worden ingestanst. Deze gegevensopslag is permanent. Bij een wijziging van de gegevens dient een nieuwe kaart aangemaakt te worden. Embossed-kaarten worden veelvuldig gebruikt in ziekenhuizen om persoonsgegevens als naam, adres, woonplaats, naam huisarts, verzekering, enz. op te slaan;
- magneet kaart: De magneetkaart is een kunststof kaart met hierop een magneetstrip aangebracht. Over het algemeen bevat deze magneetstrip een drietal sporen. Op deze sporen kunnen gegevens worden opgeslagen. De magneetkaart wordt veelvuldig toegepast voor elektronisch betalingsverkeer (creditcards, (post)bank-PIN-passen);
- optical card: De optische kaart is een geheugenkaart waarbij het principe "Write Once Read Many" (WORM) wordt toegepast. De optical card wordt daarom ook wel WORM-card genoemd. De kaart maakt gebruik van een optisch geheugen. Het is mogelijk om grote hoeveelheden gegevens op te slaan op

deze kaart. De optische kaart wordt gebruikt voor de opslag van grote documenten, zoals boekwerken en omvangrijke publikaties;

- chipcard of IC card (IC - Integrated Circuit): De chipcard is een kaart waarin één of meerdere chips zijn ingebouwd. Afhankelijk van de intelligentie die in de chip(s) is opgenomen is de volgende onderverdeling te maken:
  - memory card (geen intelligentie aanwezig);
  - smart card (memory + central processor unit (CPU));
  - super smart card (memory + CPU + display + keyboard).

Calculators

Het bezit van een calculator token is voldoende voor de identificatie van een persoon. Voor de verificatie van de identiteit van de persoon wordt, door dit token, authenticatie-informatie gegenereerd. Om de authenticatie-informatie te genereren wordt een berekening uitgevoerd waarbij gebruikgemaakt wordt van de datum en tijd op het moment van genereren en een unieke niet-reproduceerbare code. Deze niet-reproduceerbare code (PIN-code, wachtwoord - iets wat een persoon weet) wordt door de persoon ingevoerd door middel van een toetsenbord dat op het token aanwezig is. De gegenereerde authenticatie-informatie kan worden uitgelezen van het display op het token en worden ingevoerd in het toegangscontrolesysteem.

Calculator tokens worden op verschillende manieren uitgevoerd. Een aantal van deze uitvoeringsvormen kunnen worden gebruikt als een zogenaamde sleutelhanger. Ook worden super smart cards gebruikt als calculator tokens.

PCMCIA card of PC-card

In vergelijking met de smart card is de technologie die kan worden opgenomen in een PCMCIA card veel uitgebreider. De PCMCIA card heeft dezelfde omvang als een smart card met uitzondering van de dikte. Een PCMCIA card is dikker dan een smart card. De PCMCIA card wordt tegenwoordig ook wel PC-card genoemd. Er zijn 3 verschillende standaarden voor PC-cards. Kaarten van verschillende standaarden zijn niet onderling uitwisselbaar, omdat de elektronische interface niet gelijk is.

Smartdisk

De smartdisk lijkt op een standaard 3,5" floppy disk. In plaats van een magnetisch medium bevat een smartdisk elektronica in de vorm van batterijen, microprocessors en geheugenchips. met behulp van een magnetische lees/schrijf kop kan de smartdisk communiceren met een verwerkingseenheid.

Opm.: smart cards, PCMCIA cards en smartdisks worden over het algemeen gebruikt voor identificatie en authenticatie in combinatie met meerdere toepassingen. Door hun bewerkingscapaciteit en geheugencapaciteit is het mogelijk deze tokens multifunctioneel te gebruiken. De tokens worden vaak initieel gebruikt voor andere toepassingen dan identificatie en authenticatie. Gebruikersgemak, kostenbesparing

en efficiëntie zijn enkele punten die een combinatie van toepassingen (waaronder identificatie en authenticatie) mogelijk maken.

3.2 Mogelijke identificatie- en authenticatietechnieken met behulp van tokens

Tokens kunnen worden gebruikt voor identificatie. Identificatie vindt dan in de meeste gevallen plaats door:

- optische controle: bewakingspersoneel controleert het bezit en de echtheid van het token;
- elektronische controle: met behulp van randapparatuur wordt een unieke reeks van karakters die in het token is opgeslagen uitgelezen door middel van communicatie tussen token en randapparatuur. Komt deze reeks voor in de toegangscontrolelijst, dan heeft identificatie plaatsgevonden. Om aftappen van en op een later tijdstip opnieuw aanbieden van de reeks te voorkomen is het mogelijk de reeks in combinatie met de datum en tijd te bewerken met behulp van een vercijfermechanisme.

Bij het gebruik van tokens voor identificatie is authenticatie mogelijk door middel van 'iets wat een persoon weet' en/of 'iets wat een persoon is'. Naast het token dient de betreffende persoon authenticatie-informatie aan te bieden aan het toegangscontrolesysteem.

Het is niet gebruikelijk dat 'iets wat een persoon bezit' gebruikt wordt als authenticatie-informatie. Authenticatie-informatie dient namelijk niet of nauwelijks reproduceerbaar te zijn door derden. 'Iets wat een persoon bezit' kan in het bezit van derden komen (door bijvoorbeeld verlies of diefstal), waardoor de authenticatie-informatie reproduceerbaar is geworden. Dit wil echter niet zeggen dat 'iets wat een persoon bezit' niet gebruikt kan worden als authenticatie-informatie. Smarttokens daarentegen kunnen wel gebruikt worden voor controle van de authenticatie-informatie of zelfs voor het genereren van authenticatie-informatie.

In plaats van de controle van authenticatie-informatie in het toegangscontrolesysteem te laten uitvoeren is het ook mogelijk deze controle uit te voeren in een smarttoken. Deze toepassing wordt vaak gebruikt bij publieke informatiesystemen, waarbij het niet duidelijk is wie inzage heeft in vertrouwelijke informatie. Wanneer niet duidelijk is wie inzage heeft, is ook niet duidelijk of deze perso(o)n(en) te vertrouwen is/zijn. Door de controle in het token te laten plaatsvinden wordt de authenticatie-informatie afgeschermd voor derden.

Over het algemeen is authenticatie-informatie gedurende een langere periode geldig. Voor 'iets wat een persoon weet' is dit een periode die binnen een organisatie is ingesteld. Voor 'iets wat een persoon is' betekent dit dat de periode in principe gelijk is aan de levensduur van de persoon. Hoe langer deze authenticatie-

informatie geldig is, des te groter is de kans dat deze authenticatie-informatie kan worden gereproduceerd door derden.

De ideale authenticatie-informatie bestaat uit een voor derden niet-produceerbare reeks van karakters en is slechts éénmaal te gebruiken voor het verkrijgen van toegang. Dit is om opvangen en opnieuw aanbieden van de authenticatie-informatie door derden te voorkomen. De authenticatie-informatie is slechts geldig tot het moment dat toegang is verkregen tot de locatie of het informatiesysteem. Wanneer opnieuw toegang verkregen dient te worden zal een nieuwe niet-reproduceerbare reeks van karakters aangeboden moeten worden. Die niet-reproduceerbare reeks dient zowel bekend te zijn bij de betrokken persoon als in het toegangscontrolesysteem. Het genereren van die niet-reproduceerbare reeks is voor de betrokken persoon eenvoudig te realiseren met behulp van een smarttoken. Dergelijke smarttokens worden ook wel 'one-time-password generators' genoemd. Afhankelijk van hoe de niet-reproduceerbare reeks wordt gegenereerd dient de betrokken persoon een aantal handelingen uit te voeren.

Enkele voorbeelden van 'one-time-password generators' en handelingen die hierbij door de betrokken personen dienen te worden uitgevoerd zijn:

- het toegangscontrolesysteem genereert een random bitreeks. De random bitreeks wordt door de betrokken persoon ingevoerd in het token. Door het token wordt een bewerking uitgevoerd op deze bitreeks, waarbij tevens gebruik wordt gemaakt van een PIN-code die door de betrokken persoon ingevoerd dient te worden. Deze PIN-code is ook in het toegangscontrolesysteem bekend, waar dezelfde bewerking wordt uitgevoerd op de random bitreeks. De betrokken persoon voert het resultaat van de bewerking in het toegangscontrolesysteem in. Het toegangscontrolesysteem vergelijkt de resultaten van beide bewerkingen en zal al dan niet toegang verlenen aan de betrokken persoon (challenge response principe);
- het token genereert iedere keer, wanneer de betrokken persoon toegang wil tot een locatie of een informatiesysteem, nieuwe authenticatie-informatie. De authenticatie-informatie dient door de betrokken persoon aangeboden te worden aan het toegangscontrolesysteem. De generatie van de authenticatie-informatie is gerelateerd aan een volgnummer. De authenticatie-informatie dient conform de juiste volgorde aangeboden te worden aan het toegangscontrolesysteem. Om deze reden dient de betrokken persoon te weten welke volgnummers zijn gebruikt en dient hij het juiste volgnummer te gebruiken om toegang te krijgen. Deze methode is tevens te combineren met een PIN-code;
- het token genereert bijvoorbeeld iedere minuut nieuwe authenticatie-informatie. Deze informatie wordt continu op het display van het token getoond. Het token bevat hiervoor een ingebouwd tijd/datum-mechanisme. De betrokken persoon dient de authenticatie-informatie in te voeren in het toegangscontrolesysteem. Het toegangscontrolesysteem dient gesynchroniseerd te zijn en te blijven met het tijd/datum-mechanisme in het token. Tevens dient het toegangscontrolesysteem dezelfde bewerkingen als het token uit te kunnen voeren om vergelij-

kingsmateriaal, voor de aangeboden authenticatie-informatie, te kunnen genereren.

3.3 Producten en ontwikkelingen

In deze paragraaf zal kort aandacht worden besteed aan bestaande producten die gebruikmaken van tokens voor identificatie en authenticatie. Tevens zal aandacht besteed worden aan ontwikkelingen met betrekking tot gebruik van tokens voor identificatie en authenticatie. In bijlage A is een beperkt overzicht gegeven van de gevonden producten.

3.3.1 Producten

Op dit moment is een grote variatie aan producten verkrijgbaar die gebruikmaken van tokens voor identificatie en authenticatie. Een deel van dit aanbod bestaat uit producten waarmee met behulp van een token de authenticatie-informatie wordt bepaald. De rest van het aanbod bestaat uit beveiligingsproducten waar identificatie en authenticatie deel van uitmaakt. De tokens die bij deze producten gebruikt worden, hebben vaak meer functies naast de identificatie en/of authenticatie functie. Binnen dit onderzoek zal verder alleen aandacht besteed worden aan producten die gebruikmaken van tokens voor het bepalen van de authenticatie-informatie. De tokens die gebruikt worden binnen de beveiligingsproducten zijn vaak volgens dezelfde principes opgebouwd als de zelfstandig te gebruiken tokens. Hieronder vallen ook producten waarbij het token uitsluitend wordt gebruikt voor identificatie. Dergelijke tokens maken gebruik van verschillende communicatie- en beveiligingstechnieken om identificatie-informatie uit te wisselen met het toegangscontrolesysteem. Een veelvoud van dergelijke tokens is verkrijgbaar.

Per product zal een korte beschrijving worden gegeven van de functionaliteit en de wijze waarop de identificatie- en/of authenticatie-informatie tot stand komt.

©XS4U®

Het product ©XS4U® van Infinity bestaat uit meerdere kaarten op creditcard formaat. Eén van de kaarten is een transparante kunststof kaart. Op deze transparante kaart is een masker gedrukt. De overige kaarten zijn bedrukt met een matrix van cijfers en letters. Aan de rand van deze kaarten zijn coördinaten aangegeven.

Met behulp van dit product is het mogelijk om op een vrij eenvoudige wijze authenticatie-informatie te bepalen. Hiertoe dient het masker over één van de matrices gelegd te worden. Door de vorm van het masker is de authenticatie-informatie leesbaar. Door de coördinaten, die bij de positie van het masker horen, te onthouden kan de authenticatie-informatie gereproduceerd worden. Op deze manier is het mogelijk dat moeilijk te onthouden authenticatie-informatie door de betrokken persoon makkelijk te reproduceren is.

Met behulp van het product ©XS4U® is het mogelijk de authenticatie-informatie van meerdere locaties en/of informatiesystemen te bepalen.

ActivCard token

ActivCard biedt een calculator-token dat zogenaamde 'one-time-passwords' genereert. Het genereren van deze passwords gebeurt met behulp van het DES-algoritme. Tevens maakt het token gebruik van een PIN-code die door de betrokken persoon ingevoerd dient te worden om het one-time password te kunnen genereren. Met behulp van dit token kan op de volgende manieren authenticatie plaatsvinden:

- met behulp van challenge-response (asynchroon): het token berekent het password (response) naar aanleiding van een gegeven van het toegangscontrolesysteem (challenge);
- door synchronisatie met behulp van tijd of de volgorde van handelingen: het password wordt bepaald met behulp van de combinatie datum/tijd en de volgorde van handelingen. Zowel het token als het toegangscontrolesysteem dient bij te houden welke handelingen zijn uitgevoerd en dienen een goede tijdsynchronisatie te hebben met elkaar.

ActivCard biedt de mogelijkheid met één token de authenticatie voor vier verschillende toegangscontrolesystemen te regelen.

SecureID

Het SecureID token van Security Dynamics genereert iedere 60 seconden unieke, eenmalig te gebruiken onvoorspelbare toegangscodes. Het token maakt hierbij gebruik van de actuele datum en tijd en een voor ieder token unieke cryptografische sleutel. De betrokken persoon voert in het toegangscontrolesysteem zijn gebruikerscode (eventueel PIN-code) in. Hierna voert hij de door het token gegenereerde code in. Deze gegevens worden gecontroleerd met de in het toegangscontrolesysteem opgeslagen en/of gegenereerde gegevens. Hiervoor dient het toegangscontrolesysteem gesynchroniseerd te zijn met de actuele datum en tijd van het token. In het toegangscontrolesysteem wordt informatie opgeslagen om synchronisatie met de tokens te waarborgen. Deze informatie wordt regelmatig aangepast, omdat afwijkingen kunnen ontstaan tussen deze informatie en de actuele datum en tijd van de betreffende tokens.

Het token is in verschillende vormen te verkrijgen. De standaardvorm is die van een creditcard met display. Optioneel is het mogelijk het token uit te breiden met een keypad om een PIN-code in het token in te kunnen voeren. Het token met keypad kan zijn uitgevoerd in creditcard formaat (supersmart card), maar het kan ook een calculator-achtige vorm hebben.

RB-1 Challenge-Response Token

Het RB-1 token van Cryptocard is een calculator-achtig challenge response token. Het token maakt gebruik van het DES vercijferalgoritme. Het token heeft het

formaat van een creditcard en beschikt over een display en een keypad (supersmart card). Het token is te gebruiken voor authenticatie met behulp van een challenge-response en op basis van synchronisatie van handelingen. Tevens is het mogelijk met behulp van het token de toegang tot maximaal drie toegangscontrolesystemen te regelen.

Met behulp van een PIN-code en een challenge of een volgnummer van de handeling wordt door het token een unieke code gegenereerd. Deze code dient samen met een gebruikerscode in het toegangscontrolesysteem ingevoerd te worden.

SB-1 Electronic Diskette Token

Het SB-1 diskette token is eveneens van Cryptocard. Met behulp van het token wordt de toegangscontrole geregeld tot het lokale werkstation. De informatie die is opgeslagen op de harde schijf van het werkstation kan worden vercijferd met behulp van het token. Tevens kan met behulp van het token toegang worden verkregen tot host-systemen door middel van een challenge-response authenticatie. De betrokken persoon hoeft slechts één wachtwoord of PIN-code te onthouden waarmee hij het token activeert. Authenticatie voor het verkrijgen van toegang tot host-systemen wordt met behulp van challenge-response door het token zelfstandig afgehandeld.

Watchword II

Watchword II van Racal Datacom is een Calculator token dat wachtwoorden genereert door middel van een challenge-response. Om het token te activeren dient de betrokken persoon een PIN-code in te voeren.

Infocard

Infocard van Leemah DataCom Security Corporation is een creditcard formaat token met display en keypad. Met behulp van een PIN-code kan het token worden geactiveerd. Het token genereert wachtwoorden door middel van een challenge-response mechanisme.

Safeword AS

Safeword AS van Enigma Logic is een Authenticatie Server (AS) waarbij een organisatie vrij is een eigen token te selecteren die gebruikmaakt van:

- challenge-response authenticatie;
- authenticatie op basis van synchronisatie van handelingen;
- authenticatie op basis van tijdsynchronisatie.

Enigma Logic biedt zelf vier tokens die ondersteund worden door Safeword AS. Het betreft de tokens:

- DES Gold: dit is een creditcard formaat token met display en keypad. DES Gold maakt gebruik van het DES algoritme en kan wachtwoorden genereren voor maximaal 8 verschillen toegangscontrolesystemen. De betrokken persoon

dient een PIN-code in te voeren in het token. Het token authenticeert op basis van synchronisatie van handelingen;
- DES Silver: is een token van creditcard formaat met een display en een button (knop). Bij een druk op de knop genereert het token een wachtwoord;
- Safeword MultiSync;
- Safeword SofToken.

Daarnaast worden onder andere de volgende tokens door Safword AS ondersteund:
- Activcard;
- RB-1 token van Cryptocard;
- Infocard;
- Watchword.

3.3.2 Ontwikkelingen

De ontwikkelingen op het gebied van smart cards gaan nog steeds verder. Smart cards krijgen een steeds grotere verwerkingscapaciteit en grotere geheugens. Het is dan mogelijk de smart card meer en ingewikkelder bewerkingen te laten uitvoeren in kortere tijd, waardoor diverse cryptografische technieken op een smart card kunnen worden geïmplementeerd. Enkele van deze technieken zijn de zogenaamde zero knowledgement technieken en cryptografische technieken die gebruikt worden binnen de privacy enhancing technology. Tevens is het mogelijk steeds meer informatie op te slaan op een smart card. Met name het gebruik van multifunctionele smart cards zal hierdoor sterk toenemen.

Authenticatietechnieken zoals hiervoor zijn beschreven, zullen in de toekomst wellicht op één smart card gecombineerd kunnen worden met andere toepassingen en/of functionaliteit. Ook bestaat de mogelijkheid dat smart cards voor wat betreft identificatie en authenticatie de overige beschreven tokens kunnen gaan vervangen.

Er dient rekening gehouden te worden met eventuele exportbeperkingen van gebruikte cryptografische technieken. Met name producten afkomstig uit de Verenigde Staten kunnen gebonden zijn aan dergelijke exportbeperkingen. Op dit gebied zijn op dit moment ontwikkelingen gaande die leiden tot minder strenge beperkingen. Zo is recentelijk de sleutellengte van te exporteren DES-sleutels verhoogd van 40 bits naar 56 bits.

4. Identificatie en authenticatie met behulp van biometrie

Identificatie en authenticatie met behulp van biometrie is gebaseerd op 'iets wat een persoon is'. In eerste instantie zal, in paragraaf 4.1, een beschrijving van biometrie worden gegeven. Naast de eigenschappen van biometrie en de eigenschappen van het gebruik komen ook de verschillende soorten biometrische kenmerken aan de orde.

In paragraaf 4.2 zal ingegaan worden op de mogelijkheden die biometrie biedt voor identificatie en authenticatie. Tot slot zal in paragraaf 4.3 een overzicht worden gegeven van bestaande producten en ontwikkelingen.

4.1 Biometrie

Volgens het Van-Dale-woordenboek der Nederlandse taal [2] is biometrie 'het vaststellen van tel-, weeg of meetbare eigenschappen van levende wezens. In 'Identification by biometrics' [3] wordt, vrij vertaald, onder biometrie verstaan: een wetenschap uit de biologie waarbij statistiek wordt toegepast op de levende wereld.

Met biometrie kunnen op statistische wijze bepaalde gegevens worden berekend aangaande levende wezens. Enkele voorbeelden hiervan zijn:
- het berekenen van de gemiddelde leeftijd van een bepaalde bevolkingsgroep;
- het berekenen van de gemiddelde lengte van een bepaalde bevolkingsgroep;
- het berekenen van de gemiddelde groei van een bepaalde plantensoort;
- het berekenen van de gemiddelde voortplantingstijd van bepaalde diersoorten.

Door de medische wetenschap is aangetoond dat bepaalde menselijke eigenschappen voor ieder mens vrijwel uniek zijn. Deze eigenschappen kunnen fysiek zijn, zoals de vingerafdruk en gelaatstrekken. Daarnaast kunnen deze eigenschappen gebaseerd zijn op het gedrag, zoals het plaatsen van een handtekening en de toetsaanslag. De menselijke eigenschappen worden ook wel biometrische kenmerken genoemd. Biometrische kenmerken zijn te verdelen in fysieke biometrische kenmerken en biometrische gedragskenmerken.

In veel technische literatuur, aangaande (informatie)beveiliging, wordt biometrie beschreven als 'de identificatie en/of authenticatie van een levende individu met behulp van fysieke of gedragskenmerken'. Op basis van de definitie van Van Dale is dit echter niet volledig. Het gebruik van biometrische kenmerken voor identificatie en authenticatie is slechts een specifieke toepassing van biometrie. Toch zal in de rest van het rapport met biometrie bedoeld worden: de identificatie en/of authenticatie van een levende individu met behulp van fysieke of gedragskenmer-

ken. Dit is gedaan om verwarring met (eventuele) referentiebronnen en overige technische literatuur te voorkomen.

Een biometrisch kenmerk bestaat uit een verzameling van gegevens. Deze verzameling van gegevens is voor iedere individu uniek. Systemen die gebruikmaken van biometrische kenmerken transformeren de verzameling van gegevens van een biometrisch kenmerk naar een bitstroom.

Binnen de verzameling gegevens van een biometrisch kenmerk, kunnen er gegevens zijn die altijd constant zijn, maar er kunnen ook gegevens zijn die variëren. Het variëren van de gegevens wordt veroorzaakt door bepaalde factoren, zoals: omgevingsfactoren, veroudering, wijzingingen in het aanbieden van het kenmerk, stemming en beschadiging van het kenmerk. Dit kan tot gevolg hebben dat het transformeren van een biometrisch kenmerk naar een bitstroom kan variëren. Met andere woorden: twee transformaties van één uniek biometrisch kenmerk hoeven geen identieke bitstromen op te leveren. Vanuit een ander gezichtsveld bekeken kunnen twee verschillende bitstromen toch afkomstig zijn van hetzelfde unieke biometrisch kenmerk.

Bij identificatie en authenticatie met behulp van wachtwoorden wordt gebruikgemaakt van de zogenaamde één-op-één relatie. Het wachtwoord dat wordt aangeboden, dient identiek te zijn aan het wachtwoord dat in het toegangscontrolesysteem is opgeslagen. Gebruikmaken van de één-op-één relatie voor toegangscontrole met behulp van biometrische kenmerken is niet mogelijk. Er is namelijk al aangegeven dat de bitstromen niet identiek hoeven te zijn en dit is essentieel voor de één-op-één relatie. Om biometrische kenmerken toch te kunnen gebruiken voor identificatie en authenticatie dient het toegangscontrolesysteem rekening te houden met een bepaalde tolerantie bij de vergelijking van bitstromen.

4.1.1 Voor- en nadelen biometrische kenmerken

Biometrische kenmerken hebben de volgende voor- en nadelen:

- voordelen:
  - biometrische kenmerken kunnen zeer betrouwbaar zijn. De medische wereld heeft aangetoond dat sommige eigenschappen van mensen vrijwel uniek zijn. Op basis van deze eigenschappen kunnen personen geïdentificeerd worden;
  - fysieke biometrische kenmerken zijn in essentie onveranderlijk gedurende het leven;
  - biometrische gedragskenmerken kunnen in de tijd echter wel veranderen;
  - biometrische kenmerken zijn in principe niet aan derden overdraagbaar;
  - biometrische kenmerken kunnen niet worden vergeten of verloren. De kenmerken zijn altijd aanwezig;
- nadelen:
  - een wachtwoord dat niet veilig genoeg meer is, kan worden gewijzigd. Biometrische kenmerken kunnen niet veranderd worden;

- aanbieden van het biometrische kenmerk moet nauwkeurig geschieden om foute uitlezingen te voorkomen;
- matige acceptatie van identificatie en authenticatie door middel van biometrische kenmerken door gebruikers;
- het risico dat de bezitter van een kenmerk loopt, wanneer derden dit kenmerk proberen te ontvreemden. Dit risico kan worden beperkt door naast het 'meten' van het kenmerk ook bijvoorbeeld de temperatuur en de bloeddoorstroming van het kenmerk te meten.

4.1.2 Soorten biometrische kenmerken

Biometrische kenmerken zijn te verdelen in fysieke biometrische kenmerken en biometrische gedragskenmerken. Met fysieke kenmerken wordt gedoeld op lichaamskenmerken, zoals een vingerafdruk of een irispatroon. Een gedragskenmerk bestaat over het algemeen uit een combinatie van (een) fysiek(e) kenmerk(en) en psychologische kenmerken. Bij gedragskenmerken wordt echter de nadruk gelegd op de psychologische kenmerken van een persoon. Voorbeelden van gedragskenmerken zijn de dynamische handtekening of de grondtoon en klank van een stem. De volgende, zo volledig mogelijke, opsomming van fysieke en gedragskenmerken kan worden gegeven.

4.1.2.1 Fysieke kenmerken

Vingerafdruk

De karakteristiek van dit kenmerk bestaat uit herkenbare patronen van een vingerafdruk, minutiae genaamd. Dit zijn de eindpunten en kruisingen van de groefjes in de vinger. Ook kunnen andere unieke eigenschappen zoals curven en randjes die bij alle vingers voorkomen, worden gemeten. Tevens kunnen het aantal groeven tussen eindpunten of kruisingen worden gemeten. De afdruk van een vinger is in principe stabiel vanaf de geboorte. Alleen als er sprake is van (bewust of onbewust) fysiek ingrijpen, wordt de vingerafdruk gewijzigd. Denk bijvoorbeeld aan sneetjes in een vinger of een 'droge' vinger waarin kloofjes ontstaan. Tevens kunnen vuil, omgevingsomstandigheden of de plaatsing van de vinger op het venster van invloed zijn op de kwaliteit van de opname van de vingerafdruk.

Handgeometrie

Bij dit kenmerk zijn de karakteristieken gerelateerd aan de 3-dimensionale vorm van de totale hand van een persoon. Belangrijke gegevens hierbij zijn onder andere de lengte van de vingers, de dikte van de hand, de vorm van de handpalm en de helderheid van de huid. Dit kenmerk kent een goede stabiliteit vanwege het feit dat de vorm van een hand na de groeifase van een persoon niet meer fundamenteel veranderd. Net als bij de vingerafdruk geldt ook hier dat alleen door fysieke veranderingen het kenmerk zodanig gewijzigd kan worden dat een positieve verificatie niet meer te garanderen is.

Vingergeometrie
Dit kenmerk kent dezelfde karakteristieken als die van de handgeometrie met dit verschil dat nu niet de hele hand gebruikt wordt maar slechts twee vingers. De stabiliteit en betrouwbaarheid van dit kenmerk komen overeen met die van handgeometrie. Ook de werkwijze van het meten van de karakteristieken is gelijk. Een opmerkelijk verschil met de handgeometrie is dat de nu verkrijgbare apparatuur voor vingergeometrie goedkoper is dan die voor handgeometrie.

Handrugaderpatroon
Bij dit kenmerk zijn de herkenbare patronen te vinden op de rug van een hand. Het patroon van de bloedaderen op de rug van de hand is uniek voor ieder persoon. Hoe dit patroon gemeten wordt is niet precies te achterhalen, maar vermoed wordt dat het principe hetzelfde is als bij handgeometrie. De vorm van de aders plus hun patroon zijn de kenmerkende gegevens.

Handpalmafdruk
De meting van dit kenmerk berust op dezelfde techniek als gebruikt wordt voor de vingerafdruk. Er wordt bij dit kenmerk uitgegaan van de groeven in de opperhuid van de binnenkant van de hand. Het grootste verschil tussen de vingerafdruk en de handpalmafdruk is dat er niet naar één vinger gekeken wordt, maar naar de handpalm. Bij de handpalm is er in zekere zin minder sprake van karakteristieke meetpunten (eindpunten, kruisingen) van de groeven. Nu gaat het meer om de hoofdgroeven die aan de binnenkant van een menselijke hand voorkomen. Het gebruik van dit kenmerk voor biometrische identificatie wordt nog uitgebreid onderzocht. Hierdoor is er nog niet veel informatie over dit kenmerk beschikbaar.

Retinapatroon
Dit kenmerk bestaat uit gegevens afkomstig van het bloedvatenpatroon in de retina (het netvlies) achterin het oog. Het beeld dat van dit patroon gemaakt kan worden, ziet er namelijk voor ieder mens anders uit. Bij het uitlezen van de karakteristieke gegevens wordt er gebruikgemaakt van een infrarode lichtstraal met een lage intensiteit. Dit uitlezen moet wel op een goed moment gebeuren. Het is namelijk van belang dat het oog goed gepositioneerd is ten opzichte van de uitleesapparatuur en ook dat het oog *gefocust* is op een bepaald punt. Voor het uitlezen zal de lichtstraal een baan volgen om het middelpunt van het oog. Hierdoor ontstaan er reflecties die samen een beeld vormen van het aderpatroon, zoals zich dat op het netvlies bevindt. De met bloed gevulde aderen absorberen namelijk meer licht dan het witachtige weefsel er rondom heen. De stabiliteit van dit kenmerk is bijzonder goed te noemen. Het is namelijk nog nooit aangetoond dat een retinapatroon veranderd is. Het is tevens bijzonder moeilijk na te maken vanwege de vele kleine vertakkingen die zich in het patroon voordoen. Vanwege de uitzonderlijke stabiliteit en de grote uniekheid van het kenmerk is retinapatroon-verificatie één van de beste technieken, waarvan op dit moment producten op de markt zijn. Het nadeel echter is dat de gebruikersvriendelijkheid veel moet inboeten vanwege het goed positioneren en focusseren van het oog.

Irispatroon

Vanwege de geringe gebruikersacceptatie van het retinapatroon-kenmerk is het beter om een verificatiemiddel te creëren waarbij aanbieding van het kenmerk niet zo nauwkeurig hoeft te zijn. Een mogelijk kenmerk van het oog dat zich hiervoor leent, is de iris. De iris bevat enkele karakteristieke gegevens zoals rimpels, kuiltjes, ophopingen van vezels, ringen, spikkeltjes en kronkelende vaten. Doordat we hier te maken hebben met een groot aantal gegevens is de uniekheid van dit kenmerk bijzonder goed te noemen. De stabiliteit van dit kenmerk wordt geschat op tientallen jaren, lang genoeg voor praktische doeleinden. Vanwege het feit dat de iris zich aan de oppervlakte van het oog bevindt, is het niet noodzakelijk dat het oog precies gepositioneerd en scherp gesteld moet worden. Andere voordelen zijn dat de iris beschermd wordt door het hoornvlies en dat de iris niet gewijzigd kan worden zonder dat daarbij gezichtsverlies ontstaat. Het namaken van een 3-dimensionaal reliëf van het iris-oppervlak is op dit moment vrijwel ondenkbaar. Tot slot kan worden opgemerkt dat, in vergelijking met het retinapatroon, verificatie kan plaatsvinden op grotere afstand van de inleesapparatuur.

Gezichtsafbeelding

Bij mensen is het eerste herkenningspunt het aangezicht. Karakteristieken waarvan bij dit kenmerk gebruikgemaakt kan worden, zijn onder andere afstanden tussen de ogen, de haarlijn en vorm van het gezicht. Door diverse omstandigheden zal de vertoning van het kenmerk aan de camera nooit hetzelfde zijn. Zo zijn gezichtsuitdrukkingen mede afhankelijk van de stemming waarin een persoon verkeerd (blij of boos). Andere veranderingen kunnen worden veroorzaakt door haardracht, zoals bijvoorbeeld het laten staan van snorren en baarden of een veranderende haardracht. Ook verdraaiingen van het hoofd ten opzichte van vorige metingen kunnen van invloed zijn op de kwaliteit van het verificatiesysteem. Problemen kunnen zich voordoen wanneer tweelingen binnen het systeem geregistreerd staan. De karakteristieken van de kenmerken kunnen dan zoveel overeenkomen dat een valse acceptatie kan ontstaan.

Gezichtsstraling

Dit kenmerk berust op afbeeldingen van warmtepatronen die in het menselijke gezicht voorkomen. Deze patronen zijn af te leiden uit de zogenaamde gezichtsthermogrammen. Voor dit patroon wordt gebruikgemaakt van het gebied tussen de wenkbrauwen en de bovenlip. Bij ieder mens bestaan er kleine afwijkingen in het bloedvatensysteem. De afbeelding wordt verkregen door met behulp van een infraroodcamera een foto te maken en deze te digitaliseren. De uniekheid van dit kenmerk is groot. Ook is de stabiliteit van de gegevens goed te noemen. Deze methodiek is nog in ontwikkeling, waardoor er nog geen concrete gegevens over bekend zijn. Dit geldt ook voor de beschikbaarheid van commerciële producten.

Oorpatroon

Dit kenmerk bestaat uit gegevens van een menselijk oor zoals de grootte, vorm en contouren [4]. Met behulp van een videocamera wordt een plaatje gemaakt van het

oor. Er is een systeem op de markt waarbij de camera, sensoren en elektronica ingebouwd zijn in het oorgedeelte van een telefoon. Verdere gegevens over dit product of leverancier zijn niet aanwezig. Vanwege de weinige informatie is het niet duidelijk hoe het met de stabiliteit en betrouwbaarheid van dit kenmerk gesteld is. Wel zou er een goede echtheidscontrole moeten zijn, omdat een oor op zich vrij eenvoudig na te maken is. Vanwege het ietwat komisch karakter van dit kenmerk zal de acceptatie van de gebruikers vermoedelijk matig tot slecht zijn.

Lichaamsgeur
Dit kenmerk is enkele jaren geleden 'ontdekt' als bruikbaar gegeven voor identificatie en/of authenticatie. Het onderzoekstraject bij deze methodiek bevindt zich echter nog in een beginstadium, waardoor nog geen bruikbare resultaten beschikbaar zijn. Wel is bekend dat een dergelijk systeem zal moeten beschikken over een aantal sensoren die gevoelig zijn voor de aanwezigheid van specifieke geurstoffen. Uit een geurstofregistratie van een persoon wordt een persoonlijk 'odeurgram' samengesteld. Dit is een soort samenstelling van alle geurstoffen die bij de betreffende persoon voorkomen. Deze samenstelling zal naar verwachting moeilijk te vervalsen zijn, ook al zou het 'odeurgram' beïnvloed worden door het gebruik van bijvoorbeeld parfums en/of deodorants. Wel zou het 'odeurgram' beïnvloed kunnen worden als de betreffende persoon veelvuldig gebruikmaakt van andere parfums en/of deodorants. Tevens kan het 'odeurgram' worden beïnvloed door een gevarieërd eetpatroon, waarbij veel smaakmakers, zoals knofloof of kerrie, worden gebruikt.

4.1.2.2 Gedragskenmerken

Statische handtekening
De statische handtekening heeft betrekking op gegevens die afkomstig zijn van een weergave van een handtekening. Een groot probleem hierbij is dat een handtekening geen stabiele waarden in zich heeft. Zo ziet een handtekening er elke keer weer net iets anders uit. Deze kleine variaties zijn onder andere afhankelijk van de emotionele toestand of de lichaamshouding op het moment van het zetten van de handtekening. De handtekening wordt met behulp van een videocamera ingelezen. Een afbeelding van de handtekening wordt gedigitaliseerd en opgeslagen. Het verificatieproces bestaat uit het vergelijken van twee handtekeningen. Indien deze in zekere mate in optisch oogpunt overeenkomen met elkaar, is de verificatie gelukt. De betrouwbaarheid van dit kenmerk is matig te noemen. Het vervalsen van een handtekening is eenvoudig.

Dynamische handtekening

In plaats van de afbeelding van een handtekening te analyseren, is het ook mogelijk om de dynamiek van het plaatsen van een handtekening te gebruiken als biometrische toepassing. Gegevens die hierbij een belangrijke rol spelen zijn onder andere schrijfsnelheid, schrijfrichting, schrijfdikte, druk op de schrijfpen, lijnen die kruisen, totale schrijftijd, maximum hoogte, aantal lussen en aantal keren dat de pen van het papier afgehaald wordt. De meeste van de genoemde gegevens zijn niet als stabiel aan te merken. Om deze reden worden bij de systemen die nu op de markt zijn de prestaties verbeterd door na elke succesvolle verificatie de opgeslagen karakteristieken aan te passen. De systemen voor de dynamische handtekeningen die op dit moment beschikbaar zijn, werken zowel met een ontkoppelde als met een gekoppelde (draad of infrarood) pen. De variant met de ontkoppelde pen werkt in combinatie met een schrijftablet. De systemen met een gekoppelde pen werken zowel met als zonder schrijftablet. Vanuit het oogpunt van vandalisme blijven de systemen nog enigszins in gebreke, omdat altijd een pen nodig is die het systeem gevoelig maakt voor diefstal en/of moedwillige vernielingen. Net als bij de statische handtekening geldt ook hier dat het zetten van de handtekening onderhevig is aan persoonlijke invloeden zoals stress, emotie of zelfs het ouder worden van de te autoriseren persoon. Dit is tegen te gaan door na elke succesvolle autorisatie de karakteristieken aan te passen.

Grondtoon en klank van de stem

Eén van de laatst ontwikkelde, en ook de natuurlijkste vorm van biometrische herkenning is de spraakherkenning. Het kenmerk wat hierbij gebruikt wordt, is gebaseerd op de gegevens die voortkomen uit de menselijke stem. De golfvorm van een zin wordt gemeten en met behulp van een Fourier-analyse wordt het frequentiespectrum bepaald. Dit spectrum bevat de karakteristieke gegevens die benodigd zijn voor de herkenning. Voorbeelden van deze karakteristieke gegevens zijn onder andere snelheid, grondtoon, energie en de dichtheid van de golfvorm. De stabiliteit van deze karakteristieken is redelijk goed. Ook voor de mens onhoorbare frequenties worden in de analyse meegenomen, waardoor zaken als verkoudheid of humeur minder invloed uitoefenen op het frequentiespectrum. Omgevingsgeluiden kunnen wel van invloed zijn op het systeem, omdat de ruis het frequentiespectrum kan aantasten. Op het moment dat de omgevingsgeluiden veranderen, kunnen deze van grote invloed zijn op de correctheid van de autorisatie.

Typegedrag (toetsaanslag)

Een relatief nieuwe techniek is autorisatie op basis van toetsaanslag-analyse. Gegevens die van belang zijn voor het bepalen van een identiteit zijn onder andere het tijdsinterval tussen toetsaanslagen, de overlaptijd tussen toetsaanslagen, duur van een toetsaanslag en de typesnelheid. Tijdens de enrollmentfase wordt van de metingen het gemiddelde en de variatie berekend. Nader onderzoek heeft bewezen dat deze twee selectiecriteria reeds voldoende zijn voor het herkennen van personen. Toetsaanslag-analyse is één van de weinige autorisatiemethoden die continue

verificatie kan uitvoeren. De stabiliteit van het kenmerk is bijzonder goed te noemen. Externe factoren kunnen van invloed zijn op het herkenningsproces. Deze externe factoren zijn bijvoorbeeld een andere hoogte van een tafel of stoel of een omgeving waarbij de temperatuur ineens sterk veranderd is. Deze techniek staat nog in de kinderschoenen. Tegen het eind van 1996 worden de eerste commerciële producten verwacht.

4.1.3 Eigenschappen van systemen die werken op basis van biometrie

Naast de kenmerken zelf is het van belang enig inzicht te krijgen in de belangrijkste eigenschappen van systemen die biometrische kenmerken gebruiken voor de identificatie en/of authenticatie van (levende) personen. Deze eigenschappen zijn: het toepassingsgebied, de in gebruikname, het verloop van het biometrisch kenmerk, de betrouwbaarheid en tenslotte de gebruikersacceptatie van dergelijke systemen.

Toepasbaarheid

Zoals al eerder is aangegeven, wordt bij identificatie gecontroleerd of de identiteit van een persoon voorkomt op een toegangscontrolelijst. Toegangscontrole uitsluitend op basis van identificatie is een proces wat over het algemeen veel (reken)tijd kost. Tevens kunnen voor een dergelijk proces hoge eisen gesteld worden aan de rekencapaciteit van het systeem. Dit is vooral het geval als voor de identificatie gebruikgemaakt wordt van biometrische kenmerken. Biometrische kenmerken zullen dan ook voornamelijk worden toegepast voor de authenticatie (verificatie) van personen, nadat deze personen eerst op een andere manier geïdentificeerd zijn. Voor het verdere onderzoek zal worden aangenomen dat biometrische kenmerken gebruikt worden voor het verifiëren van een, op een andere manier dan met behulp van biometrische kenmerken, aangeboden identiteit.

Praktische invoering

Bij de ingebruikname van systemen die aan de hand van biometrische kenmerken personen identificeren en authenticeren, zijn twee fasen te onderscheiden. Naast de gebruiksfase is ook een fase nodig waarin de biometrische kenmerken van de betrokken personen in het systeem worden opgenomen. Deze fase wordt ook wel inleerfase of enrollmentfase genoemd, omdat het systeem de betrokken personen moet 'leren kennen'.

Vanwege de variaties in de bitstromen wordt gedurende de enrollmentfase verschillende malen het betreffende biometrische kenmerk van de betrokken persoon aangeboden aan het systeem. De enrollmentfase is belangrijk voor het bepalen van de kwaliteit van de bitstroom die opgeslagen gaat worden in het toegangscontrolesysteem. Wordt tijdens de enrollmentfase slechts één keer het biometrisch kenmerk getransformeerd naar een bitstroom, dan bestaat de kans dat de kwaliteit van deze elektronische representatie slecht is. Een slechte kwaliteit kan onder andere ontstaan door extreme omgevingsfactoren en/of het verkeerd aanbieden van het biometrische kenmerk.

Iedere keer dat het kenmerk wordt aangeboden, wordt dit kenmerk omgezet in een bitstroom. De verschillende bitstromen worden op een bepaalde manier met elkaar vergeleken. De overeenkomsten tussen de bitstromen worden gefilterd en samengevoegd, waardoor er een resultante ontstaat. De overeenkomsten worden ook wel stabiele gegevens genoemd, zie hiervoor ook [4]. Door de hoeveelheid stabiele gegevens te variëren is het mogelijk de betrouwbaarheid van een systeem te variëren.

De verkregen resultante wordt ook wel template genoemd. De template wordt opgenomen in de toegangscontrolelijst, waarna de template gebruikt kan worden voor authenticatie. De template dient uniek te zijn ten opzichte van de overige templates in de toegangscontrolelijst. Voor zover bekend is, zijn er geen standaarden voor het omzetten van biometrische kenmerken in bitstromen en het bepalen van de template. Ook worden de bestaande technieken om (bedrijfs)vertrouwelijke redenen niet prijsgegeven.

Tijdens de gebruiksfase vindt authenticatie plaats door de aangeboden authenticatie-informatie te vergelijken met de opgeslagen template. De authenticatie-informatie is gelijk aan de bitstroom die berekend wordt uit het aangeboden biometrische kenmerk.

Bij technieken op basis van kenmerken waarvan de bitstromen kunnen verlopen in de tijd, kan de opgeslagen template regelmatig worden aangepast. De opgenomen template wordt dan opnieuw bewerkt samen met de (nieuwe) authenticatie-informatie. Op deze manier wordt een nieuwe template verkregen. De 'oude' template wordt overschreven door de nieuwe template, nadat gecontroleerd is dat de nieuwe template uniek is ten opzichte van de overige, in de toegangscontrolelijst opgenomen, templates.

Verloop van het biometrisch kenmerk

Er is reeds geconstateerd dat 'metingen' aan biometrische kenmerken kunnen variëren. Deze variaties worden voornamelijk veroorzaakt door omgevingsfactoren. Ook kunnen biometrische kenmerken zelf wijzigen. Door veroudering, beschadiging of stemmingen kunnen biometrische kenmerken aan veranderingen onderhevig zijn. Veroudering en beschadiging kunnen worden opgevangen door de template aan te passen met (nieuwe) authenticatie-informatie. Opgemerkt dient te worden dat bij beschadiging ook de gevoeligheid van de apparatuur voor stof, vuil en dergelijke wordt ondergebracht.

Met name stemmingen en omgevingsfactoren zorgen voor variaties waar niet of nauwelijks op kan worden ingespeeld. Omgevingsfactoren, zoals sterke temperatuurvariaties en een sterk vervuilde omgeving kunnen ervoor zorgen dat de metingen, die verricht worden, worden beïnvloed. Stemmingen en modeverschijnselen, zoals stress, baardgroei en haardracht, zorgen er eveneens voor dat metingen kunnen worden beïnvloed.

Het is dus zaak biometrische kenmerken te selecteren voor specifieke toepassingen die zo min mogelijk afhankelijk zijn (of invloed ondervinden) van de bij deze toepassingen horende omgevingscondities.

Betrouwbaarheid van systemen die werken met biometrie

Voor systemen die biometrische kenmerken gebruiken voor verificatiedoeleinden kan op twee manieren naar betrouwbaarheid worden gekeken. De eerste manier veronderstelt dat het systeem is blootgesteld aan dreigingen en tegenstanders of opponenten. Deze beschouwing zal in het volgende hoofdstuk verder worden uitgewerkt. Ook de begrippen dreigingen en tegenstanders zullen hier nader worden verklaard. De tweede manier veronderstelt dat het systeem niet wordt blootgesteld aan dreigingen en tegenstanders anders dan de dreiging dat ongeautoriseerde personen toegang proberen te krijgen door 'gewoon proberen'. Het systeem is als het ware werkzaam onder 'normale' omstandigheden. Voor het gemak zal deze visie van betrouwbaarheid worden aangeduid als 'de betrouwbaarheid van de verificatiemethode'.

De betrouwbaarheid van de verificatiemethode kan worden afgeleid uit de hoeveelheid ongewenste acceptaties van ongeautoriseerde personen en de hoeveelheid ongewenste afwijzingen van geautoriseerde personen. De ongewenste acceptatie van ongeautoriseerde personen en de ongewenste afwijzing van geautoriseerde personen worden vaak uitgedrukt in percentages. Deze percentages worden aangeduid met False Acceptance Rate (FAR) voor ongewenste acceptaties en False Rejection Rate (FRR) voor ongewenste afwijzingen. De FAR en FRR zeggen echter niets over de betrouwbaarheid van het systeem zelf (met andere woorden: is het systeem veilig geïmplementeerd).

Eerder is aangegeven dat het aantal stabiele gegevens dat gebruikt wordt voor het bepalen van de template invloed uitoefent op de betrouwbaarheid van een systeem. De FAR en FRR worden beïnvloed door het variëren van het aantal stabiele gegevens. Zo zal bij het gebruik van meer stabiele gegevens de FAR kleiner worden en de FRR groter worden en vice versa. Een hoge FAR geeft een minder betrouwbare methode, maar geeft wel een grotere gebruikersacceptatie. Het is ook mogelijk de betrouwbaarheid te verbeteren door hoge eisen te stellen aan de enrollmentfase. Dit geeft een betere kwaliteit van de template, waardoor een betere waarde van de FAR en FRR ontstaat.

Een aantal van de op dit moment verkrijgbare systemen heeft een vaste waarde voor de FAR en FRR. Het aantal te vergelijken stabiele gegevens ligt bij dergelijke systemen vast. Er zijn ook systemen op de markt verkrijgbaar waarvan het aantal stabiele gegevens is in te stellen. Hierdoor zijn verschillende combinaties van FAR en FRR mogelijk.

Gebruikersacceptatie

Het succes van authenticatie door middel van een biometrisch kenmerk is naast de prestaties, betrouwbaarheid en stabiliteit mede afhankelijk van de acceptatie van de gebruiker.

Eén aspect van de gebruikersacceptatie is het gebruiksgemak. Hierbij gaat het om slechts één enkele vraag; hoe eenvoudig is het apparaat te gebruiken? Gebruiksgemak kan voor wat betreft biometrie worden opgesplitst in een aantal factoren. Eén van die factoren betreft de manier waarop het biometrisch kenmerk aan het apparaat moet worden aangeboden. De handeling moet voor de gebruiker op een natuurlijke manier verlopen en mag hem niet afschrikken. Tevens moet het aanbieden van het kenmerk slechts op één manier kunnen gebeuren. Een andere factor heeft betrekking op de tijd die nodig is voor het verificatieproces. Deze moet binnen een aanvaardbare tijdsduur liggen om ergernis bij de gebruikers te voorkomen.

Een ander aspect van gebruikersacceptatie heeft betrekking op de risico's die de bezitter van een kenmerk loopt. Deze risico's hebben betrekking op de ontvreemding van de identificatie- en/of authenticatie-informatie door tegenstanders. Een tegenstander kan op een aantal manieren in het bezit komen van deze informatie. Voor 'iets wat een persoon is', oftewel biometrische kenmerken, betekent dit dat een kenmerk geamputeerd kan worden. Een andere mogelijkheid is dat een tegenstander onder dwang het gebruik van een kenmerk afdwingt. In beide gevallen zal het slachtoffer hieraan ernstige fysieke en/of emontionele schade overhouden. Dergelijke risico's en gevolgen kunnen worden teruggedrongen door de verificatie-apparatuur een aantal controlemetingen uit te laten voeren. Zo zou de temperatuur en de bloeddoorstroming van het kenmerk gemeten kunnen worden.

Voorstanders van het gebruik van gedragskenmerken beweren dat beveiliging op basis van deze kenmerken beter geaccepteerd wordt dan systemen die gebruikmaken van fysieke kenmerken. Deze bewering berust op een tweetal veronderstellingen. De eerste is dat beveiligingssystemen met gedragskenmerken als minder opdringerig zouden worden ervaren. De tweede veronderstelling is dat het verifiëren van de menselijke handtekening of stem veel dichter bij de mensen zou staan, omdat deze kenmerken sociaal constant gebruikt en geaccepteerd worden.

Uit een onderzoek van de *Australian National University* [5] is gebleken dat de hierboven genoemde bewering geen correcte afspiegeling van de werkelijkheid weergeeft. De globale conclusies uit het onderzoek zijn dat alle, op dat moment, bestaande systemen gekenschetst worden als minder acceptabel dan de traditionele systemen gebaseerd op wachtwoord-beveiliging. Tegen alle verwachtingen in is gebleken dat de systemen gebaseerd op gedragskenmerken minder geaccepteerd worden dan de systemen die gebruikmaken van fysieke kenmerken. De algemene acceptatie van biometrische kenmerken wordt groter naar mate de gevoeligheid van de te beschermen informatie ook groter wordt. Dit in tegenstelling tot de

relatie tussen acceptatie van wachtwoord-systemen en gevoeligheid van de te beschermen informatie.

Het zal duidelijk zijn dat het niet eenvoudig is om een goed onderbouwde uitspraak te doen omtrent de gebruikersacceptatie van de diverse producten zonder zelf eerst met die producten in aanraking te zijn geweest. Hoe een bepaald product of technologie in een grote groep mensen ervaren wordt, is nooit met 100 % zekerheid te voorspellen.

4.2 Mogelijke identificatie en authenticatie technieken met behulp van biometrie

Biometrie wordt, zoals al eerder is aangegeven, voornamelijk gebruikt voor de verificatie van de identiteit van een persoon. Hierbij is het mogelijk biometrische kenmerken te gebruiken voor incidentele toegangscontrole en voor periodieke of continue toegangscontrole. In principe zijn alle biometrische kenmerken geschikt voor incidentele toegangscontrole. Fysieke kenmerken lenen zich niet of slecht voor periodieke of continue toegangscontrole. Bij fysieke kenmerken is het namelijk belangrijk dat het kenmerk juist gepositioneerd wordt. Dit positioneren kan hinderlijk zijn wanneer dit vaak of continu dient te gebeuren. Gedragskenmerken, zoals toetsaanslag, zijn uitermate geschikt voor continue verificatie van gebruikers.

4.3 Producten en ontwikkelingen

In deze paragraaf zal worden aangegeven welke producten, die gebruikmaken van biometrische kenmerken voor identificatie en authenticatie, commercieel verkrijgbaar zijn. Per kenmerk zal daar waar mogelijk een opsomming en korte beschrijving van de te leveren producten worden gegeven. Tevens zal aandacht besteed worden aan eventuele ontwikkelingen van technieken en/of producten. Geprobeerd is een zo volledig mogelijke opsomming te geven van commercieel verkrijgbare producten. Voor een aantal kenmerken bestaan wel al producten, maar deze zijn nog niet commercieel verkrijgbaar. Indien voldoende informatie beschikbaar is, zullen deze producten ook beschreven worden. Van kenmerken die niet meer worden genoemd, is geen informatie over producten beschikbaar. In bijlage B is een beperkt overzicht gegeven van de gevonden producten. Hierbij is tevens een kostenindicatie gegeven.

Vingerafdruk

Van dit kenmerk zijn de volgende producten commercieel verkrijgbaar:

TouchSafe II

Dit product is afkomstig van Identix Inc. uit Californië USA. Het systeem bestaat uit een kastje waarop een transparante plaat is gemonteerd, waar de gebruiker zijn vinger op legt. In het kastje zit de hardware en ander aanverwante zaken zoals de vinger-uitleesapparatuur en het vergelijkingsalgoritme. Met behulp van een parallelle aansluiting wordt het kastje verbonden met een PC door middel van een standaard printplaatje die in elk 16 bits ISA-slot past. De template die tijdens de enrollmentfase aangemaakt wordt, is ongeveer 1200 bytes groot. Desgewenst kan ervoor gekozen worden dat er nog een tweede template aangemaakt wordt van een andere vinger zodat men in geval van verwondingen aan de eerste vinger terug kan vallen op deze tweede template.

Het proces dat door dit product wordt uitgevoerd is een identificatie-proces. De tijd die de enrollment-fase in beslag neemt is ongeveer 35 seconden (alleen het opnemen van 3 vingerafdrukken). De tijd die voor de identificatie zelf nodig is, bedraagt 0,5 tot 1 seconde. Voordat het systeem echter gedetecteerd heeft of de vinger goed geplaatst is, is er een seconde verstreken. Identificatie kost dus ongeveer 2 seconden.

FingerCheck

Dit product is afkomstig van Startek Engineering uit Taiwan. Dit systeem kent net als touchsafe een venster waarop de vinger geplaatst dient te worden. Tevens bezit het systeem ook twee verhoogde steuntjes, om te zorgen dat de vingertop iedere keer weer goed geplaatst wordt. Tijdens de enrollmentfase worden er drie afdrukken genomen van een bepaalde vinger. Deze drie afdrukken vormen dan één template van zo'n 256 bytes. Deze template kan zowel op een computer maar ook op een token opgeslagen worden. Hiervoor is dan wel een aparte unit vereist die ook door Startek geleverd wordt. Dit systeem kent vijf vooraf ingebedde beveiligingsinstellingen. Deze onderscheiden zich van elkaar door steeds andere waarden voor de parameters van FAR en FRR. De scantijd van het inlezen van het kenmerk bedraagt 1/30 seconde, terwijl de verificatietijd in totaliteit ongeveer 2 tot 3 seconden in beslag zal nemen.

Andere producenten/leveranciers op het gebied van vingerafdruk zijn onder andere:

- Printrak International uit Californië USA (verdere informatie is niet bekend);
- IAS Enterprise; Deze levert het AFIM-systeem waarbij een kaartlezer ingebouwd is. Dit zijn magneetstrip kaarten.
- Mytec Technologies Inc. levert het Zebra True Recognition System. Ook deze bezit een ingebouwde kaartlezer, waarbij ook optische kaarten en smart cards ondersteund worden. Mytec claimt dat het op een geheel andere manier komt tot een uiteindelijke template. Ze werken namelijk niet met herkenningspunten maar met een afbeelding van de gehele vingerafdruk. Deze wordt optisch gescand, gecomprimeerd en opgeslagen.
- Morpho uit Frankrijk (verdere informatie is niet bekend).

De meeste van deze producten zijn qua functionaliteit gelijk aan elkaar. De methoden om tot een template te komen zijn allemaal gebaseerd op dezelfde manier. Hoe men **precies** aan de template komt, wordt echter door geen enkele producent vrijgegeven.

Handgeometrie

Voor dit kenmerk is eigenlijk maar één commercieel product verkrijgbaar, namelijk het ID3D Handkey van Recognition Systems Inc. uit de Verenigde Staten. Het systeem bestaat uit een behuizing waarin aan één zijde een hand geplaatst kan worden. Met behulp van een camera en een spiegeltje worden zowel de bovenzijde als de weerszijden van de hand gescand. Om ervoor te zorgen dat de hand steeds weer op de goede manier geplaatst wordt, zijn er een aantal geleidepinnen in het kastje aangebracht waarlangs de vingers geplaatst moeten worden.

De template die door het systeem aangemaakt wordt, is slechts 9 bytes groot. Deze template wordt in combinatie met een gebruikerscode opgeslagen in het geheugen van het systeem of op een token. Het geheugen van het apparaat zelf biedt plaats aan maximaal 20.000 templates, afhankelijk van de grootte van het geïnstalleerd geheugen. Voor de verificatie wordt gebruikgemaakt van een *stand alone*-unit. De handkey-unit kan zowel in *stand alone*-omgevingen als in *online*-omgevingen werken. Na een verificatie geeft de ID3D een waarde terug die tussen 0 en 255 ligt. Bij 0 is er geen enkele afwijking gevonden tussen de aangeboden hand en de template, terwijl hogere waarden afwijkingen aangeven. Meestal wordt er een drempelwaarde gekozen die tussen 25 (streng) en 75 (minder streng) ligt.

De verificatietijd ligt tussen de 1 en de 2 seconden. De tijd die nodig is voor het goed plaatsen van de hand en de vingers zal in de praktijk ongeveer 2 tot 3 seconden zijn.

Vingergeometrie

Van het Zwitserse bedrijf BioMet Partners is in 1994 het product *Digi-2* op de markt gebracht. De gebruikers kunnen zelf de twee vingers kiezen die ze willen gebruiken voor de verificatieprocedure. De eenmaal gekozen vingers zullen dan wel altijd gebruikt moeten worden. De template die afkomstig is van een 3-dimensionale opname van de vingers kan opgeslagen worden op een token, in het geheugen van het apparaat of in het geheugen van een computer. De template is 20 bytes groot. Het geheugen van het apparaat biedt plaats aan duizend templates.

BioMet levert het product niet als een compleet systeem, maar heeft besloten om het als 3 losse onderdelen te verkopen. Zo is er het optische chassis, de opto-electronica en de printplaten, die doorgaans gemakkelijk in bestaande apparatuur in te bouwen zijn. De tijd om de vingers op de juiste plek te plaatsen zal, afhankelijk van de ervaring, ongeveer twee tot drie seconden in beslag nemen. De tijd die benodigd is voor de verificatie van een persoon bedraagt ongeveer één seconde.

Handrugaderpatroon

Voor dit kenmerk zijn nog geen commerciële producten verkrijgbaar. Wel zijn er aanwijzingen dat er in Japan vergevorderde ontwikkelingen zijn, omdat handgeometrie door de Japanse cultuur slecht wordt geaccepteerd. Vermoedelijk zullen dus ook vanuit Japan de eerste producten op de markt komen.

Handpalmafdruk

Ook voor dit kenmerk zijn er nog geen commercieel verkrijgbare producten beschikbaar en er is niet bekend of binnenkort producten op de markt komen. Verdere informatie is eveneens niet beschikbaar.

Retinapatroon

EyeDentify Inc. is de enige producent van een systeem welke gebaseerd is op het kenmerk van het retinapatroon. Het laatst gelanceerde product is het EyeDentification System 2001. Het systeem bevat een apparaat waarmee het aderpatroon op het netvlies kan worden gescand en waar ook een key-pad met display op is gemonteerd. Het apparaat heeft een ingebouwd geheugen welke plaats biedt aan ongeveer 3000 templates van 96 bytes elk. Het systeem kijkt naar 400 voorgeprogrammeerde referentiepunten. Deze worden verder geanalyseerd en gecomprimeerd tot 192 referentiepunten en opgeslagen in de eerder genoemde templates. De templates kunnen ook opgeslagen worden op diverse soorten tokens.

De gebruiker dient bij het verificatieproces eerst een gebruikerscode in te voeren, zodat zijn template reeds in het werkgeheugen wordt geladen. Daarna plaatst de gebruiker zijn oog voor het daarvoor ontworpen ooggedeelte. Voor de verificatie is het noodzakelijk dat het oog goed gefocusseerd wordt. Dit gebeurt door middel van een oplichtend puntje in het apparaat waar de gebruiker naar dient te kijken. Het apparaat neemt dan met behulp van een infrarood licht het aderpatroon op. Het gebruik van de gebruikerscode is niet strikt noodzakelijk want het systeem kan ook het gepresenteerde patroon vergelijken met alle geregistreerde templates. Het zal duidelijk zijn dat dit proces (identificatie-proces) nu enkele seconden langer zal duren. Tot slot nog een opmerking omtrent de montage van het apparaat; het is leverbaar in een monteerbare versie (voor montage in muren), maar ook in een draagbare versie.

De tijd die nodig is voor de verificatie van een persoon bedraagt ongeveer 1,5 seconde. Het herkennen van een template uit de database van alle opgeslagen templates kost iets minder dan 5 seconden. Het feit dat het oog goed gepositioneerd en gefocused moet worden, zal zeker van invloed zijn op de tijd die in zijn totaliteit nodig is voor het verifiëren van een persoon. Deze tijd zal dan ook sterk afhankelijk zijn van de ervarenheid van de gebruikers.

Irispatroon

Het enige product wat nu op de markt is voor irisherkenning is "IriScan 2000 EAC" van IriScan Inc.. Met behulp van een normale camera wordt een opname gemaakt van het oog. Hiertoe dient de gebruiker op een kleine afstand van de camera te staan. Focussen van het oog is niet noodzakelijk bij dit kenmerk. Met een video frame grabber wordt de opname geanalyseerd, gecomprimeerd en vervolgens wordt de file opgeslagen als een template van 512 bytes.

Het systeem bepaalt tijdens de enrollment-fase zelf hoeveel keer een opname gemaakt moet worden, voordat er een goede en betrouwbare template is ontstaan. Nadeel van dit systeem is dat de training die voor de verificatie benodigd is, niet eenvoudig is. De camera moet goed voor het oog geplaatst worden, omdat anders niet het volledige oog op de opname terecht komt.

In zijn algemeenheid kan gemeld worden dat bij dit product een tijd van ongeveer twee seconden benodigd is om een persoon te verifiëren of te identificeren. De tijden zijn wel afhankelijk van de verwerkingskracht van de interne processor van de computer.

Gezichtsafbeelding

Voor het kenmerk gezichtsafbeelding zijn een viertal producten verkrijgbaar. De producenten/leveranciers zijn: BAeSEMA, Facia Reco, Miros Inc. en NeuroMetric Vision Systems. Het TrueFace systeem van Miros Inc. is één van die 4 commerciele producten. Dit systeem maakt gebruik van neurale netwerk technologie om de gepresenteerde afbeelding te vergelijken met de afbeelding die reeds in een template is opgeslagen in het systeem.

Als de gebruikte frame grabber snel genoeg is, is het niet noodzakelijk dat de gebruiker precies stil hoeft te staan. Ook is de afstand tot de apparatuur variabel zolang het gezicht maar in het opnameveld ligt. Het systeem is ook niet gevoelig voor hoofddraaiingen van minder dan 20° naar links of rechts en 20° naar boven of beneden. De afbeelding van het gezicht wordt "gevangen" door de camera en vervolgens gecomprimeerd tot een file van 500 bytes die zowel in het systeemgeheugen als op een token opgeslagen kan worden. Het systeem is niet gevoelig voor onder andere haarstijl, wel of geen bril en natuurlijke kleuring van de huid.

Er moet rekening gehouden worden met een verificatietijd van 1,5 seonde. Hier komen over het algemeen geen extra tijden meer bij, omdat de camera altijd wel redelijk goed opgesteld staat.

Gezichtsstraling

Van identificatie en/of authenticatie op basis van dit kenmerk is slechts weinig informatie voor handen. Er is wel een bedrijf dat bezig is met een commercieel product, namelijk Technology Recognition Systems (TRS) uit Virginia USA. Verdere informatie omtrent deze ontwikkeling ontbreekt.

Statische handtekening

Authenticatiesystemen, die gebruikmaken van een statische handtekening, worden door dezelfde producenten van dynamische handtekening verificatiesystemen op de markt gezet. Deze producten werken allemaal volgens eenzelfde principe namelijk het vergelijken van twee gescande handtekeningen. Een voorbeeld van een product is "Chequematch" van AEA Technology uit de United Kingdom. Bij dit product wordt een scanner meegeleverd waarmee de gezette handtekening wordt gescand. Vervolgens wordt deze scan vergeleken met de opgeslagen template van de handtekening van dezelfde persoon.

Chequematch kan zowel voor identificatie als voor verificatie gebruikt worden. Ook zijn er mogelijkheden zoals *cheque clearing*, *credit agreement processing* en *payment slips*. Dit zijn hulpmiddelen die veel gebruikt worden in de financiële wereld. Hiermee wordt direct de grootste toepassingsmarkt duidelijk, namelijk de bedrijfsprocessen waar veel financiële afhandelingen worden verricht. Een andere succesvolle producent van een statische handtekening verificatiesysteem is IBM, dat het product SIVAL/2 op de markt heeft gebracht.

Omtrent deze producten zijn geen performance gegevens beschikbaar en worden door de producent ook niet vermeld in de tot nu toe uitgebrachte literatuur.

Dynamische handtekening

Op dit moment zijn er ongeveer 10 commerciële producten op de markt die de identiteit van een persoon kunnen verifiëren door de dynamiek van het zetten van een handtekening te analyseren. Dit zijn onder andere de volgende producenten: Checkmate Electronics, IBM, Xenetek, Peripheral Vision. Ook AEA Technology levert een dergelijk product, namelijk: Countermatch. Het systeem bestaat uit een tablet en een softwareprogramma. Tijdens de enrollment-fase dient de gebruiker drie maal zijn handtekening te zetten en het systeem analyseert op welke wijze de persoon zijn handtekening zet. Vervolgens wordt aan de hand van die analyse een template gevormd van 1000 bytes groot. Deze template wordt opgeslagen in de PC samen met een gebruikerscode.

Tijdens de verificatie wordt aan de hand van de gebruikerscode de juiste template in het werkgeheugen geladen en vervolgens vergeleken met de gepresenteerde handtekening. Het systeem maakt gebruik van de neurale netwerk technologie voor het uitvoeren van de vergelijkingen. Het resultaat van een vergelijking is een getal tussen nul en één. Een nul is het resultaat bij een vergelijking zonder enige verschillen en een één is het resultaat van een vergelijking met alleen maar verschillen.

Ook hier geldt dat er geen gegevens omtrent performance bekend zijn.

Grondtoon en klank van de stem

Producten die gebaseerd zijn op de technologie van het analyseren van de menselijke stem worden onder andere geproduceerd door Marconi, International Electronics Inc., Texas Instruments en Domain Dynamics en nog enkele anderen. Bij de "VoiceKey" van International Electronics Inc. wordt het stempatroon opgeslagen samen met een gebruikerscode. Het systeem is ontworpen voor *stand alone*-gebruik bij fysieke toegangscontrole. VoiceKey bestaat uit een, in een beveiligde ruimte opgestelde, controller en een bij de deur gemonteerde gebruikersterminal. De user interface van deze terminal bestaat uit een display, keypad, microfoon en indicatielampjes.

Voor de enrollment-fase moet de gebruiker een wachtwoord kiezen dat hij drie maal in de microfoon moet inspreken. Het systeem maakt dan een template aan en zal deze beveiligen met een gebruikerscode. Het toevoegen/wijzigen van gebruikerstemplates is beveiligd met een wachtwoord dat alleen bij de beveiligingsfunctionaris bekend hoort te zijn. Verificatie gaat aan de hand van de gebruikerscode die de gebruiker eerst aan het systeem bekend moet maken. Zodra de gele LED gaat branden, kan de gebruiker het wachtwoord in de microfoon inspreken. Zodra de verificatie geslaagd is, zal de opgeslagen template aangepast worden. Als de verificatie mislukt, moet de gebruiker opnieuw het wachtwoord inspreken. De totale verificatietijd bedraagt gemiddeld zo'n 6,5 seconden.

Ook Alpha Microsystem uit California USA, levert producten die werken met dit kenmerk. Zo leverde het bedrijf eerst het Voxtron-systeem. Nu is er een nieuwe versie beschikbaar die uitgebracht wordt onder de naam Ver-A-Tel. Dit systeem maakt gebruik van een PC welke de hardware en software bevat. De "user terminal" is uitgevoerd als een normaal druk-toets-telefoon. De software ondersteunt de benodigde beheersfuncties voor de enrollment- en gebruiksfase.

Tijdens de enrollment-fase zal een beveiligingsfunctionaris voor iedere gebruiker een persoonsrecord aanmaken. Dit record wordt voorzien van een unieke gebruikerscode. De software is ook nog voorzien van een aparte code om het enrollment-proces te starten zodat de enrollment-fase van een ongeautoriseerd persoon kan worden tegen gegaan. Tijdens de enrollment-fase moet een gezegde gekozen worden dat de persoon wil gebruiken tijdens de verificatie. Dit gezegde kan gekozen worden uit een reeks van voorbeelden, maar ook een "eigen" gezegde is mogelijk.

Zowel bij de enrollment- als bij de verificatiefase moet men eerst via de telefoon een verbinding opbouwen met de PC. Vervolgens wordt de gebruiker geacht om zijn 4-cijferige gebruikerscode in te geven op de keypad van de telefoon. Tijdens de enrollment moet de gebruiker nu een aantal malen achter elkaar een gezegde noemen. Zodra het systeem vindt dat alle uitspraken genoeg op elkaar lijken, worden de gegevens opgeslagen en verwerkt tot een template. Tijdens de verificatie wordt de gebruiker verzocht om zijn gezegde te noemen en zal aan de hand van

de correctheid wel of niet worden geautoriseerd. De tijd die benodigd is voor de verificatie van een persoon bedraagt gemiddeld zo'n 19,5 seconde.

De verwachting is dat de meeste producenten doorgaan met het verder ontwikkelen van dergelijke producten, want uit verschillende bronnen blijkt dat deze producten goed aanslaan.

Typegedrag (toetsaanslag)

Trave Investments uit Canada zal dit jaar met twee producten op de markt komen, Biopassword in het tweede gedeelte van 1996 en een afgeleide ervan tegen het eind van 1996. Het product Biopassword biedt de mogelijkheid tot eenmalige verificatie, terwijl het afgeleide product tevens de continue verificatie zal kunnen uitvoeren.

Op de Universiteit van Bradford in het Verenigd Koninkrijk heeft men een systeem ontwikkeld welke continue verificatie van een gebruiker kan uitvoeren.

Ook bij TNO-FEL [6] is onderzoek verricht aan deze verificatietechniek. Dit onderzoek heeft geresulteerd in een demonstrator, waarmee personen continu geïdentificeerd en geauthenticeerd kunnen worden.

De verwachting is dat er in de nabije toekomst meer van dergelijke systemen worden ontwikkeld. Deze producten bestaan voornamelijk uit software wat als bijkomend voordeel heeft dat het goedkoop kan zijn.

5. Gecombineerd gebruik van tokens en biometrie

Tot nu toe heeft het onderzoek zich toegespitst op het afzonderlijk bestuderen van tokens en biometrie zonder een combinatie van de twee technieken in beschouwing te nemen. Gezien de ontwikkeling van de smart card komt ook de combinatie van tokens en biometrie steeds dichterbij. In dit hoofdstuk zal dan ook aandacht worden besteed aan de mogelijkheden om tokens en biometrische kenmerken te combineren en de ontwikkelingen op dit gebied aan te geven.

5.1 Mogelijkheden

Zoals al is beschreven in hoofdstuk 2 zijn voor identificatie en authenticatie minimaal twee gegevens nodig. Op dit moment is het mogelijk een token te gebruiken voor identificatie en een biometrisch kenmerk voor authenticatie.

Bij deze combinatie is het mogelijk onderscheid te maken in de plaats waar de template van het biometrisch kenmerk is opgeslagen. De template kan zijn opgeslagen in een centrale toegangscontrolelijst behorende bij het toegangscontrolesysteem. De template kan ook zijn opgeslagen in het token zelf.

Daarnaast kan onderscheid gemaakt worden naar waar de authenticatie-informatie wordt vergeleken met de opgeslagen template. Dit kan plaatsvinden in het toegangscontrolesysteem. Over het algemeen is het zo dat het toegangscontrolesysteem de betrokken personen niet vertrouwt. Het kan echter ook voorkomen dat de betrokken persoon het toegangscontrolesysteem niet vertrouwt, bijvoorbeeld als dit toegangscontrolesysteem behoort bij een publiek informatiesysteem. Vanuit dit standpunt van de betrokken persoon is het wenselijk dat de vergelijking van de authenticatie-informatie en de template in het token plaatsvindt.

Resumerend levert dit de volgende uitvoeringsvormen op, waarbij het token wordt gebruikt voor de identificatie en het biometrisch kenmerk voor de authenticatie:

1. de authenticatie-informatie wordt in het toegangscontrolesysteem vergeleken met de in het toegangscontrolesysteem bij de betreffende identiteit opgeslagen template;
2. de authenticatie-informatie wordt in het toegangscontrolesysteem vergeleken met de in het token opgeslagen template. Hiervoor dient de template van het token naar het toegangscontrolesysteem getransporteerd te worden. Voordeel van deze vorm ten opzichte van de vorige vorm is dat er in de toegangscontrolelijst geen templates hoeven te worden bijgehouden;
3. de authenticatie-informatie wordt in het token vergeleken met de in het token opgeslagen template. In feite werkt deze manier van authenticeren als volgt: de betrokken persoon voert zijn token in in het toegangscontrolesysteem. Hiermee identificeert hij zichzelf. Met behulp van een biometrisch kenmerk wordt in het

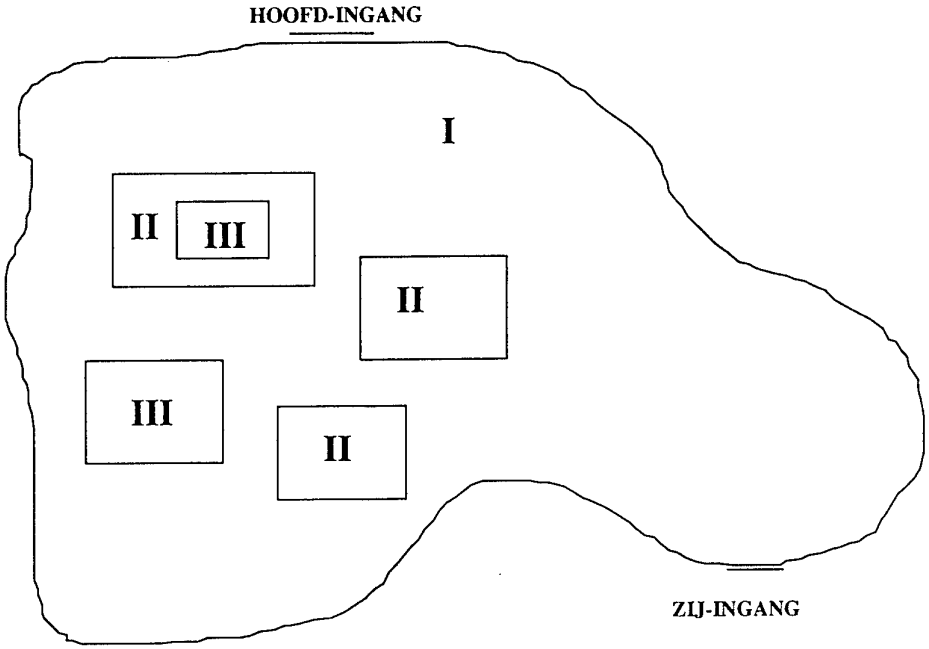
token bepaald of deze persoon is wie hij beweert te zijn. Nadat deze bewerking is uitgevoerd, wordt aan het toegangscontrolesysteem doorgegeven of de persoon wel of niet is wie hij beweert te zijn. Met deze methode is het voor derden niet of nauwelijks mogelijk om de authenticatie-informatie te bemachtigen. Het toegangscontrolesysteem dient echter wel vertrouwen te hebben in de werking en echtheid van het token.

Opgemerkt dient te worden dat uitvoeringsvorm 'de authenticatie-informatie wordt in het token vergeleken met de in het toegangscontrolesysteem opgeslagen template' niet is genoemd. Reden om de vergelijking door het token te laten uitvoeren is dat het toegangscontrolesysteem niet wordt vertrouwd. Wanneer dit het geval is, is het ook niet raadzaam de template op te slaan in een toegangscontrolelijst.

Afhankelijk van de eisen die gesteld worden aan de te beschermen locatie en/of het te beschermen informatiesysteem kan gekozen worden voor één van de voorgaande uitvoeringsvormen. Om dit te verduidelijken is in figuur 5.1 een fictieve locatie weergegeven. Binnen deze locatie zijn een aantal gebieden te onderscheiden. Deze gebieden onderscheiden zich van elkaar door de verschillende beveiligingseisen die aan deze gebieden gesteld worden. In figuur 5.1 zijn deze gebieden genummerd van I t/m III.

Gebied I heeft betrekking op dat deel van de locatie waaraan minimale beveiligingseisen gesteld worden. In dit geval geeft gebied I het terrein binnen de omheiningen aan. Gebied II is het gebied waaraan gemiddelde beveiligingseisen gesteld worden. Dit kunnen bijvoorbeeld gebouwen zijn die zich op binnen de omheining van gebied I bevinden. Gebied III heeft betrekking op het gebied waaraan maximale beveiligingseisen gesteld worden. Een dergelijk gebied is bijvoorbeeld een extra beveiligde verdieping of afdeling van een gebouw of een in zijn geheel extra beveiligd gebouw.

Bij het verstrekken van toegang tot gebied I dient een deel van het toegangscontrolesysteem, namelijk de randapparatuur, buiten de gecontroleerde omgeving opgesteld te worden. Geautoriseerde personen kunnen niet controleren of de randapparatuur is gemanipuleerd. De organisatie kan wellicht eisen dat de ingangen van de locatie extra bewaakt worden door bewakingspersoneel of observatiecamera's, om manipulatie van de randapparatuur te voorkomen. Is dit echter niet mogelijk, dan zou hier vanuit het standpunt van de geautoriseerde personen het beste uitvoeringsvorm 3 gebruikt kunnen worden.



Figuur 5.1: Schematische weergave van een mogelijke indeling van een locatie in beveiligingsgebieden

Voor gebied II en gebied III als voor informatiesystemen kan worden verondersteld dat het gehele toegangscontrolesysteem zich bevindt binnen een gecontroleerde omgeving. Voor deze gebieden en informatiesystemen kunnen zowel uitvoeringsvorm 1 als uitvoeringsvorm 2 in aanmerking komen. Afhankelijk van de te treffen beveiligings- en beheermaatregelen dient gekozen te worden voor één van deze 2 uitvoeringsvormen.

5.2 Ontwikkelingen

Bij diverse producten die gebruikmaken van biometrische verificatie worden tokens geleverd voor de identificatie. Momenteel worden tokens nog niet gebruikt voor het vergelijken van authenticatie-informatie (het gemeten kenmerk) en de template.

Met PCMCIA-cards en Smartdisks is het mogelijk het token zelf vergelijkingen van kenmerken en templates uit te laten voeren. Smart cards beschikken op dit moment nog niet over voldoende verwerkingcapaciteit om een dergelijke vergelijking zelfstandig uit te kunnen voeren. In de nabije toekomst zal hier waarschijnlijk verandering in komen, zodat deze vergelijking ook met een smart card mogelijk is.

6. Dreigingsscenario's (aanvalspaden)

Om een beter inzicht te krijgen in de betrouwbaarheid van bestaande producten, is in dit onderzoek gekozen voor het bestuderen van het gedrag van deze producten bij blootstelling aan dreigingen die voor de KLu relevant zijn. Deze dreigingen zullen in dit hoofdstuk nader bepaald worden.

Een definitie van een dreiging is de volgende: een mogelijke gebeurtenis die een ongewenst effect heeft op het beschouwde systeem. Een dreiging kan verder worden uitgewerkt door in beschouwing te nemen wie of wat de dreiging kan veroorzaken. Hierbij wordt gesproken over een zogenaamde tegenstander of opponent. Hierdoor wordt het mogelijk een nauwkeuriger inschatting te maken van de waarschijnlijkheid van optreden van dreigingen. De maatschappelijke plaats van de organisatie bepaalt de motieven van de tegenstanders. Ook kan de maatschappelijke positie van de organisatie bepaalde tegenstanders uitsluiten of aantrekken. Door tegenstanders te koppelen aan dreigingen en een beschrijving te geven van mogelijke handelingen ontstaan concrete dreigingsscenario's.

In de eerste paragraaf van dit hoofdstuk zal dieper ingegaan worden op de tegenstanders. De beschrijving van tegenstanders is binnen het Ministerie van Defensie ook wel bekend als daderprofiel. In paragraaf 6.2 zal dieper ingegaan worden op relevante dreigingen. Tot slot zal in paragraaf 6.3 een aantal scenario's worden opgesteld, waaraan een selectie van producten zal worden blootgesteld.

6.1 Tegenstanders en daderprofiel

Door de Binnenlandse Veiligheids Dienst (BVD) en de Militaire Inlichtingen Dienst (MID) is een daderprofiel opgesteld voor potentiële tegenstanders. Dit daderprofiel gaat uit van een drietal categorieën daders. Deze categorieën zijn:

- outsiders; de daders of tegenstanders werken niet binnen het Ministerie van Defensie;
- insiders; de daders of tegenstanders zijn werkzaam voor het Ministerie van Defensie dan wel behoren tot personeel van derden die werkzaam zijn op een locatie binnen het Ministerie van Defensie, zoals bijvoorbeeld aannemers, schoonmaakpersoneel;
- outsiders die geholpen worden door insiders.

Binnen de categorieën worden voor het Ministerie van Defensie twee typen daders onderkend. Deze typen zijn:

- de crimineel gemotiveerde daders. Hieronder vallen onder andere: baldadige jeugd, amateur of gelegenheidsdaders, semi-beroeps of gewoonte-misdadiger en beroepsmisdadiger. De crimineel gemotiveerde dader volgt vaak een specifieke wijze van optreden;

- de politiek gemotiveerde daders. De politieke dader is verder onder te verdelen in tegenstander type I en tegenstander type II. Tegenstanders van het type I zijn personen of groepen van personen die als doelstelling hebben door middel van allerlei acties tegen defensiecomplexen en materieel de aandacht te trekken van pers en publiek. De verschijningsvormen van hun activiteiten zijn in het kader van actievoeren: demonstratie, bezetting en blokkade. Tegenstanders van het type II zijn personen of groepen van personen die zich tegen de krijgsmacht in Nederland richten naar aanleiding van het optreden van Nederlandse strijdkrachten in het buitenland.

Een onderzoek naar daders kan worden verdiept door de modus operandi, waaronder deze daders dreigingen uitvoeren, te beschouwen. Met behulp van deze modus operandi is de kans dat een dader de dreiging ten uitvoer zal brengen te bepalen. Punten waarmee deze modus operandi kan worden bepaald zijn:

- middelen: dit heeft betrekking op de middelen die een dader ter beschikking heeft om een dreiging tot uitvoer te brengen. Middelen kunnen zijn: gereedschappen, wapens, geld, kennis of ervaring;
- motivatie: dit heeft betrekking op de reden waarom een dader een dreiging wil uitvoeren. Hierbij zijn politieke-, religieuze overtuiging, afpersing of omkoping enkele voorbeelden;
- gelegenheid: dit heeft betrekking op de mogelijkheid om een dreiging uit te voeren.

In overleg met de opdrachtgever zijn de volgende invullingen gegeven voor de modus operandi van de verschillende typen daders:

- voor criminele daders geldt dat ze kunnen beschikken over geld, wapens, gereedschappen, kennis, technische vaardigheden, ervaring en mankracht (middelen). De motivatie is gericht op geldelijk gewin (buit, beloning) en kan worden afgedwongen met behulp van chantage of bedreiging. De gelegenheid is bij deze dader wel aanwezig, maar zal zich beperken door genomen maatregelen en de tijdsdruk behorende bij geldelijk gewin. Aanvullend hierop kan voor zogenaamde 'hackers' gesteld worden dat de motivatie berust op persoonlijke bevrediging, zoals intellectuele uitdaging, pret en wraakneming. Tevens kan gesteld worden dat de 'hacker' beschikt over voldoende tijd (gelegenheid);
- voor politiek gemotiveerde daders geldt dat ze beschikken over mankracht (middelen) en tijd (gelegenheid). De motivatie is natuurlijk gebaseerd op politieke overtuiging.

6.2 Relevante dreigingen

Zoals eerder is aangegeven, luidt de definitie van een dreiging als volgt: een mogelijke gebeurtenis die een ongewenst effect heeft op het beschouwde systeem. Verondersteld kan worden dat er oneindig veel gebeurtenissen zijn die ongewenste effecten kunnen hebben op het betreffende systeem. Een analyse van het systeem

zal dan een oneindig proces worden. Om dit te voorkomen dienen dreigingen geanalyseerd te worden. Tijdens een dergelijke analyse wordt onder andere onderzocht of een dreiging kan worden uitgevoerd door een onderkende tegenstander. Ook wordt tijdens zo'n analyse onderzocht of een dreiging veel of weinig risico's vormt voor het systeem en/of de organisatie.

De volgende dreigingen in relatie tot tokens en biometrie kunnen worden onderkend (hoe de dreigingen verlopen en door wie ze worden uitgevoerd zal binnen de paragraaf scenario's worden beschreven):

- verlies van het token;
- diefstal van het token;
- vervalsing (namaak/kopie) van het token, de enrollment, het biometrisch kenmerk en/of van templates;
- beschadiging van het token en/of het kenmerk;
- moedwillige beschadiging/vernieling de randapparatuur;
- opvangen en herhalen van verzonden authenticatie-informatie (replay transmissie);
- onder dwang afstaan van identificatie- en/of authenticatie-informatie;
- dubbelganger (dit geldt specifiek voor biometrie).

In overleg met de opdrachtgever is bepaald dat geen van de dreigingen ten uitvoer wordt gebracht door personen werkzaam binnen de organisatie (categorie II: insiders en categorie III: outsiders geholpen door insiders). Aangenomen wordt dat 'insiders' te vertrouwen zijn.

Er dient opgemerkt te worden dat in de loop van de tijd het gevormde beeld van tegenstanders en relevante dreigingen kan wijzigen. Het is dan ook belangrijk regelmatig de tegenstanders en relevante dreigingen te onderzoeken en daar waar nodig het gevormde beeld aan te passen aan nieuwe situaties en/of omstandigheden.

6.3 Mogelijke dreigingsscenario's

Van de eerder opgesomde dreigingen zijn de volgende scenario's mogelijk. De scenario's geven aan welke tegenstander van toepassing is. Tevens wordt in het scenario opgenomen wat de middelen, motivatie en gelegenheden zijn van de betreffende tegenstander. Bij het gebruik van middelen door criminele daders zal altijd gekeken worden of de dreiging meer oplevert dan dat door de dader geïnvesteerd moet worden om de dreiging uit te kunnen voeren.

Verlies van het token

Een defensiemedewerker verliest zijn token in een ongecontroleerde omgeving. Zowel de politiek georiënteerde dader als de criminele dader kunnen het token vinden. Tevens kunnen ze het token herkennen aan de hand van de organisatiege-

gevens die op het token staan vermeld. Er wordt verondersteld dat er een meldingsprocedure bestaat voor de defensiemedewerker als deze constateert dat hij/zij het token heeft verloren. Tevens wordt verondersteld dat PIN-codes, wachtwoorden en/of andere authenticatie-informatie niet in het bezit zijn van de dader.

Voor de politiek georiënteerde dader type I geldt dat:
- hij niet beschikt over voldoende middelen om het token nader te onderzoeken, waardoor hij uitsluitend uitwendig onderzoek kan verrichten aan het token;
- hij het token kan uitproberen op defensielocaties die vrij toegankelijk zijn en waar de juiste randapparatuur opgesteld staat;
- hij, als het token uitsluitend voor identificatie wordt gebruikt, vrij toegang heeft tot defensielocaties of systemen;
- hij, als naast identificatie ook authenticatie wordt toegepast, bij toeval (na het raden van de authenticatie-informatie) toegang heeft tot defensielocaties of systemen.

Voor de politiek georiënteerde dader type II en de criminele dader geldt dat:
- de baldadige jeugd, de amateur of gelegenheidsdader en de vandaal kunnen worden vergeleken met de politiek georiënteerde dader type I;
- de semi-beroeps of beroepsmisdadiger de beschikking heeft over voldoende middelen om het token zowel uitwendig als inwendig uitgebreid te onderzoeken;
- de semi-beroeps of beroepsmisdadiger weet (na onderzoek) hoe het token geconfigureerd is;
- de semi-beroeps of beroepsmisdadiger zonder toeval toegang heeft tot een deel van de defensielocaties en/of systemen zolang het token niet geregistreerd staat als vermist/verloren.

Diefstal van het token

De politiek georiënteerde dader en de baldadige jeugd zullen een token slechts dan ontvreemden als ze daartoe de gelegenheid hebben. In veel gevallen betreft het dan tokens die aan de aandacht van de defensiemedewerker zijn ontglipt. Het token is bijvoorbeeld blijven liggen op een bureau, in een dashboardkastje, op het dashboard of in een koffer die wordt opengebroken of ontvreemd.

De kans bestaat dat eventuele authenticatie-informatie tegelijkertijd met het token wordt ontvreemd. Dit hoeft echter niet het geval te zijn. De kans dat een token in combinatie met de authenticatie-informatie wordt ontvreemd is reëel, maar zal niet groot zijn.

Criminele daders (uitgezonderd baldadige jeugd) die voldoende gemotiveerd zijn om tokens te ontvreemden zullen vrijwel altijd hun doel bereiken. Ook tokens die worden beschermd kunnen door deze daders worden ontvreemd.

Ook hier bestaat de kans dat tegelijkertijd met de ontvreemding van het token authenticatie-informatie wordt ontvreemd. De dader heeft daarnaast voldoende middelen ter beschikking voor het achterhalen van de authenticatie-informatie, wanneer deze niet eenvoudig is te ontvreemden.

Wanneer de tokens in het bezit zijn van de daders, gelden verder dezelfde gegevens als bij het scenario 'verlies van het token'.

Vervalsing van het token

Voor de vervalsing van tokens is kennis van de technologie vereist. Daarnaast is het noodzakelijk de juiste apparatuur te gebruiken. Vervalsing van tokens is een dreiging die voornamelijk door criminele daders zal worden uitgevoerd. Deze daders hebben hiertoe de beschikking over de juiste middelen, om zowel het fysiek van het token als de logische inhoud van het token te vervalsen. Wanneer een token vervalst is, geldt dat de dader, zonder dat hij veel problemen hoeft te verwachten, toegang heeft tot de lokatie of het informatiesysteem.

Vervalsing van het biometrisch kenmerk

Voor het vervalsen van biometrische kenmerken zijn technieken nodig die vakmanschap vereisen. Een aantal biometrische kenmerken is goed te vervalsen. Er is echter wel een afdruk van het kenmerk nodig om het kenmerk te kunnen vervalsen. Voor andere kenmerken geldt dat ze minder makkelijk te vervalsen zijn. Bijvoorbeeld: het kenmerk gezichtsafbeelding is met cosmetica op het eerste gezicht goed te vervalsen. Echter de geometrische verhoudingen van gezichten is met cosmetica niet of nauwelijks te wijzigen. Met plastische chirurgie is echter wel wijziging van de geometrie mogelijk, maar zal niet altijd het gewenste effect geven.

Gezien het feit dat biometrie het best gebruikt kan worden voor authenticatie zal de dader ook over een (valse) identiteit dienen te beschikken voor het verkrijgen van toegang. Deze dreiging treedt dan ook alleen op in combinatie met één van de dreigingen met betrekking tot tokens.

Vervalsing van templates (enrollmentfase)

Ook hier geldt dat de dreiging alleen in combinatie met een andere dreiging kan worden uitgevoerd. De dader heeft toegang gekregen tot de locatie waar de enrollmentfase wordt uitgevoerd. Deze toegang heeft hij gekregen door gebruik te maken van een verloren, gestolen of vervalst token. Tevens dient de dader een niet van echt te onderscheiden legitimatiebewijs bij zich te hebben.

De dader zal zich melden bij het organisatie-element dat zorgdraagt voor de enrollmentfase. Wanneer niet gedetecteerd wordt dat de dader onbevoegd is, zal van deze dader een template worden gemaakt. Deze template zal worden toegevoegd aan de toegangscontrolelijst van het toegangscontrolesysteem.

Beschadiging van het token en/of het kenmerk

Door bewuste of onbewuste handelingen kan een token of kenmerk beschadigen. Deze dreiging heeft in eerste instantie slechts weinig gevolgen voor de organisatie. Voor de gebruiker heeft deze dreiging echter meer gevolgen. Een beschadigd token of kenmerk kan leiden tot het weigeren van toegang tot een locatie op een informatiesysteem. Als een dergelijke dreiging veelvuldig optreedt, kan dit acceptatieproblemen geven. Als dit het geval is, heeft de dreiging wel degelijk gevolgen voor de organisatie.

Er is aangenomen dat daders behorende tot categorie II geen dreigingen ten uitvoer brengen. Deze dreiging is hier echter een uitzondering op. Deze dreiging wordt voornamelijk ten uitvoer gebracht door het personeel (de gebruiker van het token of het kenmerk) van de organisatie zelf.

Moedwillige beschadiging/vernieling van de randapparatuur

De daders die een dergelijke dreiging zullen uitvoeren behoren tot de baldadige jeugd, vandalen of politiek georiënteerde daders. De motivatie van de daders is voornamelijk gericht op het zoveel mogelijk toebrengen van schade aan de organisatie.

Er wordt verondersteld dat deze daders slechts die apparatuur kunnen benaderen die aan de buitenkant van een locatie staat opgesteld, zoals het geval is bij toegangspoorten.

Opvangen en herhalen van verzonden identificatie- en/of authenticatie-informatie (replay transmissie)

Voor het uitvoeren van deze dreiging zijn middelen nodig in de vorm van de juiste apparatuur en kennis. De semi-beroeps en beroepsmisdadiger worden als potentiele daders gezien.

Deze dreiging kan op zichzelf staan wanneer tokens gebruikmaken van contactloze communicatie. Wordt echter geen gebruikgemaakt van contactloze communicatie, dan dient de dader tevens over het (vervalste) token (identificatie-informatie) te beschikken om de opgevangen informatie opnieuw uit te zenden. Voor opnieuw uitzenden van informatie die betrekking heeft op biometrische kenmerken dient de dader tevens te beschikken over de identificatie-informatie.

Onder dwang afstaan van identificatie- en/of authenticatie-informatie

Bij deze dreiging is het in principe mogelijk dat zowel de criminele dader als de politiek georiënteerde dader deze dreiging ten uitvoer brengt. Afhankelijk van de motivatie zal een gebruiker identificatie- en/of authenticatie-informatie afstaan. Dit kan zijn doordat de gebruiker wordt gechanteerd of bedreigd.

Een dader kan op deze manier toegang krijgen tot een locatie of een informatiesysteem zonder dat hiervoor identificatie- en authenticatie-informatie hoeft te worden vervalst.

Dubbelganger (specifiek voor biometrie)

Het is mogelijk dat verschillende personen beschikken over biometrische kenmerken, waarvan de karakteristieken zo weinig verschillen dat vergelijkingen van kenmerken en templates valse acceptaties (FAR) kunnen veroorzaken. Een dergelijke dreiging kan bij toeval optreden, maar het is ook mogelijk dat door criminele daders gezocht wordt naar personen met vrijwel identieke kenmerken.

Bij deze dreiging geldt dat de dreiging in combinatie met een andere dreiging zal worden uitgevoerd. Naast het gelijkende kenmerk is ook identificatie-informatie nodig om geaccepteerd te worden. Als dreigingen voor deze combinatie zijn mogelijk:

- verlies van het token;
- diefstal van het token;
- vervalsing van het token;
- opvangen en herhalen van verzonden identificatie- en/of authenticatie-informatie (replay transmissie);
- onder dwang afstaan van identificatie- en/of authenticatie-informatie.

7. Toetsing van selectie van producten aan de scenario's

In de voorgaande hoofdstukken is een aantal producten beschreven. Om een globale indruk te krijgen van de betrouwbaarheid van deze producten zal in dit hoofdstuk worden getracht deze producten te toetsen aan de onderkende dreigingsscenario's.

De toetsing is slechts een eerste orde benadering op basis van beschikbare informatie, die in sommige gevallen summier is. Het is derhalve mogelijk dat de resultaten van de toetsing enigszins afwijken van de werkelijkheid.

Er is bij het toetsen verondersteld dat het toegangscontrolesysteem zich bevindt in een gecontroleerde omgeving. Het toegangscontrolesysteem wordt als voldoende beveiligd beschouwd. Wel kan het zijn dat uitleesapparatuur van tokens en/of biometrische kenmerken zijn opgesteld buiten de gecontroleerde omgeving. Hierbij is het mogelijk, voor een tegenstander, informatie op te vangen en bijvoorbeeld opnieuw aan te bieden aan de uitleesapparatuur.

Uit het onderzoek is gebleken dat een aantal dreigingen geen directe gevolgen heeft op de werking van de te toetsen producten. Deze dreigingen zijn:
- moedwillige beschadiging/vernieling van de randapparatuur;
- onder dwang afstaan van identificatie- en/of authenticatie-informatie, en;
- opvangen en herhalen van verzonden identificatie- en/of authenticaite-informatie (replay transmissie).

De dreiging 'moedwillige beschadiging/vernieling van de randapparatuur' beïnvloedt voornamelijk de beschikbaarheid van het toegangscontrolesysteem. De betrouwbaarheid van het toegangscontrolesysteem wordt nauwelijks aangetast door deze dreiging. Door extra maatregelen te treffen kan de beschikbaarheid van het toegangscontrolesysteem worden verbeterd. Enkele voorbeelden van maatregelen zijn:
- een veelvoud van randapparatuur plaatsen, zodat op meerdere plaatsen toegang kan worden verkregen;
- alleen tamperproof randapparatuur plaatsen;
- de randapparatuur inbouwen in infrastructurele voorzieningen, waardoor deze dreiging minder invloed heeft op de apparatuur.

Voor de bescherming van personeel dient bij het optreden van de dreiging 'onder dwang afstaan van identificatie- en/of authenticatie-informatie' een aantal organisatorische maatregelen genomen te worden. Eén van de oplossingen hiervoor is het instellen van een noodprocedure. Deze noodprocedure heeft twee doelen. Het eerste doel is te zorgen dat onbevoegde personen geen toegang wordt verstrekt. Het tweede doel betreft de veiligheid van de persoon die onder dwang wordt gehouden. In plaats van het aanbieden van de gebruikelijke identificatie- of au-

thenticatie-informatie kan het slachtoffer zogenaamde nood-informatie aan het toegangscontrolesysteem aanbieden. Bij het aanbieden van de nood-informatie wordt het bewakingspersoneel gealarmeerd. De nood-informatie dient bij de dader de indruk te wekken dat de toegang wordt toegekend, zodat deze geen argwaan krijgt. De noodprocedure dient ook te voorzien in maatregelen die het slachtoffer beschermen tegen de dader, wanneer deze ontdekt dat zijn plannen zijn doorzien.

De dreiging 'Opvangen en herhalen van verzonden identificatie- en/of authenticaite-informatie' heeft alleen betrekking op producten die buiten het gecontroleerde gebied zijn opgesteld. Verondersteld wordt dat deze dreiging niet binnen het gecontroleerde gebied zal optreden. Voor communicatie tussen tokens en randapparatuur buiten het gecontroleerde gebied is de dreiging relevant. Voor producten die gebruikmaken van biometrische kenmerken is de dreiging niet relevant, omdat verondersteld wordt dat deze producten niet buiten het gecontroleerde gebied worden geplaatst.

In eerste instantie zijn de tokens getoetst aan de dreigingsscenario's. De resultaten zijn weergegeven in de eerste paragraaf van dit hoofdstuk. Daarna zijn de producten die biometrische kenmerken gebruiken voor identificatie en/of authenticatie getoetst. De resultaten hiervan zijn weergegeven in paragraaf 2 van dit hoofdstuk.

7.1 Tokens

Algemeen

Bij de productbeschrijving wordt voornamelijk ingegaan op smarttokens die gebruikt worden voor het genereren van eenmalig bruikbare authenticatie-informatie. De beschreven producten zullen worden getoetst aan de relevante scenario's. In overleg met de opdrachtgever is bepaald dat de producten ©XS4U® en SB-1 Electronic Diskette Token niet zullen worden getoetst. De overige tokens die zijn beschreven zullen wel worden getoetst.

De volgende dreigingen zijn onderkend als relevant:

- verlies van het token;
- diefstal van het token;
- vervalsing van het token;
- opvangen en herhalen van verzonden identificatie- en/of authenticatie-informatie (replay transmissie).

Ook voor dumbtokens gelden de onderkende dreigingen. Verlies of diefstal kan grote gevolgen hebben voor de organisatie. Ontbrekende gegevens kunnen m.b.v. de juiste middelen eenvoudig achterhaald worden. Bijvoorbeeld gebruikersnamen (accountnamen) zijn vaak eenvoudig te achterhalen, omdat deze namen over het algemeen als bekend worden verondersteld. Voor vervalsing geldt dat dergelijke tokens m.b.v. de juiste middelen eenvoudig kunnen worden nagemaakt of geco-

piëerd. Vooral de 'replay transmissie'-dreiging is voor deze tokens van belang. Informatie die wordt uitgewisseld, tussen token en randapparatuur, is op te vangen. Doordat deze tokens zelf geen informatie kunnen genereren of manipuleren, is de identificatie- en/of authenticatie-informatie, die op het token is opgeslagen, gedurende een langere periode geldig.

Voor smarttokens geldt dat de dreiging 'opvangen en herhalen van verzonden identificatie- en/of authenticatie-informatie' wordt geminimaliseerd door het genereren van zogenaamde one-time-passwords. De gebruikte authenticatie-informatie mag worden opgevangen. Op het moment dat deze informatie opnieuw wordt aangeboden is de informatie vervallen en zal er geen toegang worden verleend. Voorkomen moet worden dat een tegenstander opvolgend meerdere malen de gegenereerde authenticatie-informatie kan opvangen. Door deze informatie te analyseren is het voor de dader wellicht mogelijk de volgende authenticatie-informatie te voorspellen.

De beschreven producten genereren op een van de volgende manieren de authenticatie-informatie door middel van een Challenge Response mechanisme, waarbij:

- de challenge een 'willekeurig' door het toegangscontrolesysteem bepaalde waarde is. Dit geldt voor de producten Activcard (optie 1), RB-1, SB-1, Watchword II en Infocard;
- de challenge is gebaseerd op het aantal keer dat door het toegangscontrolesysteem toegang is verleend aan de betreffende persoon (producten DES-gold en DES-silver);
- de challenge is gebaseerd op een, tussen het token en het toegangscontrolesysteem, gesynchroniseerde klok (product SecureID);
- de challenge is gebaseerd op een combinatie van een gesynchroniseerde klok en het aantal keer dat toegang is verleend (product Activcard (optie 2)).

Vervalsing van het token is afhankelijk van een aantal factoren. De belangrijkste factoren zijn:

- het door het toegangscontrolesysteem gebruikte mechanisme om personen te identificeren en authenticeren;
- de geschiedenis van het token. Met ander woorden: welke handelingen en bewerkingen zijn door het token uitgevoerd en welke informatie is ontvangen en/of verzonden;
- de tijdinstelling van het token en het toegangscontrolesysteem;
- de gebruikte bewerkingen (met name de gebruikte vercijferalgoritmes en sleutels).

Hoe meer van deze factoren bekend zijn hoe beter een token te vervalsen is. Aangezien de beschreven producten nagenoeg hetzelfde mechanisme gebruiken en hetzelfde vercijferalgoritme is het, met de beschikbare informatie, moeilijk te zeggen welk product makkelijker of moeilijker te vervalsen is ten opzichte van de andere producten.

Activcard

Het genereren van authenticatie-informatie is met behulp van Activcard op twee manieren mogelijk. Voor beide manieren geldt dat de gebruiker zich dient te identificeren bij het toegangscontrolesysteem. Ook dient de gebruiker een PIN-code in te voeren in het token om het token te activeren (identificeren bij het token).

Bij verlies geldt dat het token niet bruikbaar is zolang de PIN-code en de identificatie-informatie voor het toegangscontrolesysteem niet bekend zijn bij de vinder van het token. Zoals al eerder is gesteld, is de identificatie-informatie, oftewel de accountnaam, vrij eenvoudig te achterhalen, omdat deze informatie meestal algemeen bekend is. Het is dus van belang dat zorgvuldig wordt omgegaan met de PIN-code. Zijn het token en de PIN-code in het bezit van de tegenstander, dan heeft deze vrij toegang.

Voor diefstal geldt in principe hetzelfde als bij verlies. Er dient zorgvuldig omgegaan te worden met de PIN-code. Dit kan echter niet voorkomen dat PIN-code en token toch tegelijkertijd worden gestolen of onder bedreiging worden ontvreemd. Procedurele maatregelen, zoals vermelding van gestolen tokens op een zwarte lijst, zorgen ervoor dat deze dreiging tot een minimum kan worden beperkt.

SecureID

Het secureID product heeft in de standaard uitvoering geen (PIN-)code voor het activeren van het token. Bij verlies en/of diefstal hoeft nu alleen de accountnaam van de oorspronkelijke gebruiker bekend te zijn om toegang te krijgen. Optioneel is het mogelijk ook een PIN-code in te voeren in het token om dit token te activeren. Hierbij wordt de kans dat de dreiging optreedt verminderd. Zie ook het product Activcard.

RB-1 Challenge-Response Token, Watchword II en Infocard

Deze producten maken ook gebruik van een accountnaam voor het toegangscontrolesysteem en een PIN-code voor het activeren van het token. Wat betreft verlies en diefstal geldt ook hier hetzelfde als voor het product Activcard.

DES-gold/DES-silver

Het DES-gold token maakt gebruik van zowel een accountnaam voor het toegangscontrolesysteem en een PIN-code voor het activeren van het token. Ook voor het DES-gold token geldt dus hetzelfde als voor het Activcard product.

Voor het DES-silver token geldt dat het token geactiveerd wordt door middel van een druk op een, op het token aanwezige, button. De PIN-code voor het activeren van het token ontbreekt. Bij verlies of diefstal van het token is slechts een accountnaam nodig voor het verkrijgen van toegang.

7.2 Producten die gebruikmaken van biometrie

Algemeen

Veel van deze producten kunnen zowel identificeren als authenticeren. Bij de producten waar dit het geval is, zal dit worden aangegeven. Tevens zal zowel voor identificatie als voor authenticatie de scenario's worden doorlopen.

Daarnaast geldt voor veel producten dat de templates zowel decentraal als op een token opgeslagen kunnen worden. Bij veelvuldig gebruik van verificatie met behulp van hetzelfde kenmerk voor meerdere locaties en/of informatiesystemen is het raadzaam de template op te slaan op het token. De template wordt over het algemeen aangepast elke keer als het kenmerk wordt aangeboden. Bij opslag van de template op het token is altijd de meest recente template beschikbaar. Bij decentrale opslag wordt alleen die template aangepast die is opgeslagen in het betreffende toegangscontrolesysteem. In overige toegangscontrolesystemen wordt de template echter niet aangepast. Hierdoor bestaat de kans dat in toegangscontrolestystemen die minder vaak benaderd worden verouderde templates zijn opgeslagen. Dit kan tot gevolg hebben dat geautoriseerde personen worden afgewezen omdat het kenmerk te sterk is gaan afwijken van de opgeslagen template.

De volgende scenario's gelden niet voor deze producten:

- verlies van het token;
- diefstal van het token;
- vervalsing van het token.

Ook producten waarbij het gebruik van tokens tot de mogelijkheid behoort, worden niet getoetst aan deze scenario's. De tokens die door deze producten gebruikt worden, zijn niet voldoende beschreven om hierover uitspraken te doen. Geadviseerd wordt om tokens te gebruiken die in de voorgaande paragraaf wel zijn getoetst aan deze scenario's.

Verondersteld wordt dat ieder product gebruik kan maken van de mogelijkheid de enrollment-fase slechts door bevoegde personen te laten activeren. Dit is niet bij iedere productbeschrijving even duidelijk aangegeven, omdat de bestreffende informatie niet in alle gevallen toereikend is. Om ervoor te zorgen dat onbevoegde personen de enrollment-fase kunnen activeren dient een zorgvuldige functiescheiding, met de daarbij behorende (organisatorische) maatregelen, te worden ingevoerd.

Vingerafdruk

Het product touchsafe II is alleen te gebruiken voor identificatie. Vervalsing van het kenmerk zal dan ook toegang bieden tot locaties of informatiesystemen. Een vingerafdruk is relatief eenvoudig te vervalsen. Een vervalsing kan gemaakt worden door een afgietsel te maken van het te vervalsen kenmerk. Van dit afgietsel kan een kenmerk worden gereproduceerd op een dunne laag siliconen. Deze dunne

laag siliconen wordt op een vinger geplakt en kan worden aangeboden voor identificatie.

Bij beschadiging van het kenmerk is de kans groot dat geautoriseerde personen de toegang wordt geweigerd. Vingers kunnen regelmatig beschadigd zijn door sneetjes, kloven of schaafwonden. Aangezien regelmatig beschadigingen kunnen optreden bij dit kenmerk, zullen geautoriseerde personen ook regelmatig worden afgewezen. Hierdoor kan de acceptatie van dit kenmerk laag zijn. Om dit probleem te ondervangen zouden twee of meer templates van verschillende vingerafdrukken per persoon opgeslagen kunnen worden. Bij beschadiging van één van de vingerafdrukken kan dan voor een andere vingerafdruk gekozen worden.

Ook de dubbelganger kan problemen veroorzaken. In hoofdstuk 4 is al beschreven dat twee verschillende kenmerken bitstromen kunnen opleveren die kunnen leiden naar dezelfde template. Door de FAR te verkleinen kunnen de gevolgen van deze dreiging worden verminderd. De FAR kan worden verkleind door het aantal meetwaarden te vergroten. Het verkleinen van de FAR heeft echter tot gevolg dat de FRR groter wordt. Dus geautoriseerde personen worden vaker afgewezen.

Voor het product Fingercheck geldt dat dit naast identificatie ook te gebruiken is voor authenticatie. Hierdoor hebben dreigingen als 'vervalsing van het kenmerk' en 'dubbelganger' minder gevolgen voor de organisatie. Geautoriseerde personen bieden namelijk eerst identificatie-informatie aan in de vorm van bijvoorbeeld een gebruikerscode of een token. Deze informatie verwijst naar de template die bij de betrokken persoon hoort. Dus naast het kenmerk is ook de identificatie-informatie nodig.

Voor de dreiging 'beschadiging van het kenmerk' geldt hetzelfde als bij het product Touchsafe II.

Handgeometrie/vingergeometrie

De betreffende producten kunnen gebruikt worden voor identificatie en voor authenticatie. Het kenmerk is aanzienlijk moeilijker te vervalsen dan een vingerafdruk. In feite dient bij een vervalsing een gehele hand nagemaakt te worden. Door de temperatuur en de bloeddoorstroming van de aangeboden hand te meten wordt het onmogelijk een kunsthand te gebruiken voor de vervalsing. Een echte hand aanpassen, zodat deze overeenkomt met de te vervalsen hand, is alleen mogelijk met geavanceerde plastische chirurgie. Als de producten gebruikt worden voor uitsluitend identificatie dan is dat met dit kenmerk 'veiliger' dan met de vingerafdruk. Dit geldt ook voor de dreiging 'dubbelganger'. Voor authenticatie geldt, net als bij het product Fingercheck, dat personen zich eerst dienen te identificeren, waarna de betreffende template wordt vergeleken met het aangeboden kenmerk.

De kans op afwijzingen bij een beschadigd kenmerk is kleiner dan bij de vingerafdruk. Bij deze producten gaat het namelijk om de omtrekken van het kenmerk.

Kleine beschadigingen (bijvoorbeeld sneetjes en kloven) hebben niet of nauwelijks invloed op het verificatieproces. Grotere, blijvende (gebroken vingers of handen, geamputeerde (delen van) vingers) beschadigingen kunnen wel gevolgen hebben voor het verificatieproces. In dat geval dient een nieuwe template gemaakt te worden. Een andere mogelijkheid is het opslaan van meerdere templates. Bij handgeometrie is het niet mogelijk van elke hand een template op te slaan, omdat de apparatuur vaak is ingesteld op slechts één van de handen. Bij vingergeometrie kan worden gekozen voor meerdere combinaties van twee vingers van dezelfde hand.

Retinapatroon/Irispatroon

Voor de producten EyeDentification System 2001 en IriScan 2000 EAC geldt in principe hetzelfde als voor de producten die gebruikmaken van handgeometrie. Het kenmerk is niet te vervalsen. Dubbelgangers kunnen worden voorkomen door eerst te identificeren en daarna te verifieren met het kenmerk. Voor verificatie is het retinapatroon van een van de ogen voldoende. Bij beschadiging zou het retinapatroon van het andere oog gebruikt kunnen worden.

Gezichtsafbeelding

Worden deze producten gebruikt voor identificatie dan geldt in principe hetzelfde als bij het product Touchsafe II. Bij gebruik voor verificatie geldt in principe hetzelfde als bij het product Fingercheck. Vervalsen van het kenmerk geeft echter aanzienlijk meer moeite dan het vervalsen van een vingerafdruk. Een namaakgezicht is niet bruikbaar, wanneer door het product ook de temperatuur en de bloeddoorstroming worden gemeten. Met behulp van grimmeerspullen en plastische chirurgie zijn eenvoudige aanpassingen te maken aan echte gezichten. Een aantal meetpunten van dit kenmerk zijn echter niet te wijzigen, zoals de afstand tussen de ogen.

Statische handtekening

De statische handtekening is relatief eenvoudig te vervalsen. Wordt het kenmerk alleen gebruikt voor identificatie dan is bij vervalsing eenvoudig toegang te verkrijgen. Wordt het kenmerk gebruikt voor verificatie dan kan deze dreiging worden verminderd.

De dreiging 'beschadiging van het kenmerk' is niet direct van toepassing. Wel is het mogelijk dat de betreffende persoon lichamelijk letsel oploopt, waardoor hij het kenmerk niet goed meer kan reproduceren. Er zal naar een alternatieve manier moeten worden gezocht om geautoriseerde personen toch toegang te verlenen.

De kans dat verschillende personen dezelfde handtekening bedenken, is zo klein dat de dreiging 'dubbelganger' niet als een dreiging wordt gezien voor dit kenmerk. Personen die moedwillig de handtekening van een andere persoon gebruiken, worden ondervangen met de dreiging 'vervalsen van het kenmerk'.

Dynamische handtekening

In tegenstelling tot de statische handtekening is de dynamische handtekening moeilijker te vervalsen. Dit zorgt ervoor dat de kans op de dreiging 'vervalsing van het kenmerk' verder wordt verminderd.

Ook hier geldt voor de dreigingen 'beschadiging van het kenmerk' en 'dubbelganger' hetzelfde als bij de statische handtekening.

Grondtoon

Met behulp van een cassette-recorder is het mogelijk de gesproken woorden of gezegden op te nemen en op een later tijdstip aan te bieden aan het toegangscontrolesysteem. Omdat het hier gaat om verificatie dient ook de gebruikerscode voor de identificatie bekend te zijn om het toegangscontrolesysteem te misleiden. Om vervalsing tegen te gaan, zouden tijdens de enrollment-fase meerdere woorden of gezegden ingesproken kunnen worden. Tijdens het verificatieproces kan dan door het systeem worden aangegeven welk woord of gezegde dient te worden aangeboden. Door het toegangscontrolesysteem wordt willekeurig bepaald welk woord of gezegde ingesproken moet worden. Door naast het kenmerk ook de reactietijd te meten kan worden voorkomen dat een tegenstander het woord of gezegde kan opzoeken op de cassette.

Ook hier geldt dat de dreiging 'beschadiging van het kenmerk' niet direct zal voorkomen. Door problemen met de keel of de stembanden bestaat de mogelijkheid dat het kenmerk (tijdelijk) wordt aangetast. Ook hier geldt dat een alternatieve manier voor het verkrijgen van toegang aanwezig dient te zijn.

De dreiging 'dubbelganger' wordt beperkt door de gebruikerscode.

Typegedrag

Van dit kenmerk en de producten is te weinig bekend om een oordeel te geven over de mogelijkheid het kenmerk te vervalsen.

Hier geldt voor de dreiging 'beschadiging van het kenmerk' hetzelfde als bij de statische handtekening.

De dreiging 'dubbelganger' wordt beperkt door het kenmerk uitsluitend te gebruiken voor verificatie van de identiteit.

8. Conclusies en aanbevelingen

In dit hoofdstuk worden de conclusies en aanbevelingen die voortvloeien uit het onderzoek beschreven.

8.1 Conclusies

Een token dat gebruikt wordt voor identificatie of het genereren van authenticatie-informatie maakt deel uit van een toegangscontrolesysteem. Dergelijke tokens dienen uitsluitend aan geautoriseerde personen uitgegeven te worden.

Tokens zijn gevoelig voor verlies of diefstal en dienen daarom niet gebruikt te worden als authenticatie-informatie.

Smarttokens kunnen zelf bewerkingen uitvoeren, waardoor ze gebruikt kunnen worden wanneer:
- de organisatie waarmee gecommuniceerd wordt niet kan worden vertrouwd;
- de randapparatuur waarmee wordt gecommuniceerd niet kan worden vertrouwd.

Tokens kunnen gebruikt worden voor:
- identificatie:
  - optische identificatie;
  - elektronische identificatie;
  - elektronische identificatie gevolgd door authenticatie door middel van 'iets wat een persoon weet' of 'iets wat een persoon is';
- het genereren van authenticatie-informatie.

Smart cards zijn tokens die op dit moment nog steeds in ontwikkeling zijn. Deze ontwikkelingen hebben betrekking op het vergroten van de verwerkingscapaciteit en de bruikbare geheugenruimte. Ook zijn er ontwikkelingen gaande op het gebied van multifunctionele smart cards.

Het gebruik van biometrische kenmerken heeft de volgende voor- en nadelen:
- voordelen:
  - biometrische kenmerken zijn over het algemeen zeer betrouwbaar;
  - fysieke biometrische kenmerken zijn in essentie onveranderlijk gedurende het leven;
  - biometrische kenmerken zijn in principe niet aan derden overdraagbaar;
  - biometrische kenmerken kunnen niet worden vergeten of verloren;
- nadelen:
  - biometrische kenmerken kunnen niet veranderd worden;
  - aanbieden van het biometrische kenmerk moet nauwkeurig gebeuren;

- matige acceptatie van biometrische kenmerken;
- het risico dat de bezitter van een kenmerk loopt, wanneer derden dit kenmerk proberen te ontvreemden.

Op dit moment worden om technische redenen biometrische kenmerken voornamelijk gebruikt voor authenticatie.

Tijdens de enrollment-fase is het belangrijk dat er een template wordt gemaakt met een goede kwaliteit.

De betrouwbaarheid van een systeem dat gebruikmaakt van biometrische kenmerken wordt aangegeven met de 'False Acceptance Rate' (FAR) en de 'False Rejection Rate' (FRR). Een hoge FAR geeft een minder betrouwbare methode, maar heeft een hoge gebruikersacceptatie. Een hoge FRR geeft een betrouwbare methode, maar heeft een lage gebruikersacceptatie tot gevolg.

De gebruikersacceptatie is afhankelijk van:
- gebruiksgemak;
- risico's voor de bezitters van het kenmerk.

Beveiligingsgebieden van diverse gradaties zijn af te dekken door het gebruik van tokens in combinatie met wachtwoorden en/of biometrische kenmerken. Deze combinaties kunnen zich voordoen in diverse toepassings- of uitvoeringsvormen van tokens en bepaalde biometrische kenmerken.

De gegevens met betrekking tot prestaties van de meeste producten die gebruikmaken van biometrische kenmerken zijn gebaseerd op proefopstellingen onder ideale omstandigheden (laboratoriumopstellingen). De producten dienen derhalve nog uitontwikkeld te worden.

Een aanzienlijk deel van de relevante dreigingen is via procedurele maatregelen af te vangen. Deze dreigingen zijn niet te beïnvloeden door de gebruikte techniek van de getoetste producten.

Voor smarttokens die met behulp van een PIN-code geactiveerd dienen te worden, zijn veiliger dan smarttokens die niet geactiveerd hoeven te worden.

De biometrische kenmerken retinapatroon en irispatroon zijn niet of nauwelijks te vervalsen. Hierdoor zijn deze kenmerken het meest betrouwbaar. De meetmethode vereist echter dat het kenmerk nauwkeurig aangeboden dient te worden. Dit heeft tot gevolg dat eventuele producten niet voldoende worden geaccepteerd.

De kenmerken vingerafdruk, statische en dynamische handtekening zijn relatief eenvoudig te vervalsen, maar hebben een hoge gebruikersacceptatie.

De kenmerken handgeometrie en vingergeometrie zijn aanzienlijk moeilijker te vervalsen dan de vingerafdruk. De gebruikersacceptatie is daarentegen goed te noemen. Op dit moment verdienen producten die gebruikmaken van de kenmerken handgeometrie en vingergeometrie de voorkeur boven producten die gebruikmaken van andere kenmerken.

8.2 Aanbevelingen

Wanneer het vertrouwen in bepaalde delen van het toegangscontrolesysteem vergroot dient te worden, wordt aanbevolen smarttokens te gebruiken voor het genereren van eenmalig te gebruiken authenticatie-informatie. Delen van het toegangscontrolesysteem die eventueel hiervoor in aanmerking komen zijn bijvoorbeeld de randapparatuur voor het uitlezen van de identificatie- en/of authenticatie-informatie die is opgesteld buiten het gecontroleerde gebied.

Deze aanbeveling geldt ook als geautoriseerde personen communiceren met een organisatie die niet wordt vertrouwd.

Om de gevolgen van verlies of diefstal te verminderen wordt aanbevolen dumbtokens uitsluitend te gebruiken voor identificatie, wanneer dit gecombineerd wordt met authenticatie, door 'iets wat een persoon weet' of 'iets wat een persoon is'.

Aangezien de toetsing van de producten is gebaseerd op beperkte (commerciële) informatie, is het aan te bevelen deze producten in de praktijk te onderzoeken en te testen. Tijdens het testen van producten dient ook gekeken te worden naar de diverse combinatiemogelijkheden van tokens en biometrische kenmerken. Hierbij zal gezocht moeten worden naar combinaties, waarbij de combinatie van betrouwbaarheid en gebruikersacceptatie de beste prestatie geven.

9. Verklarende woordenlijst

Authenticatie:
De handeling van het verifieren van de geclaimde identiteit van een entiteit

Authenticatie informatie:
Informatie die gebruikt wordt voor het valideren van de geclaimde identiteit

Beschikbaarheid:
De mate waarin een informatiesysteem in bedrijf is op het moment dat de organisatie het nodig heeft

Biometrie:
- Het vaststellen van tel-, weeg of meetbare eigenschappen van levende wezens (Van Dale)
- Een wetenschap uit de biologie waarbij statistiek wordt toegepast op de levende wereld (Identification by biometrics)
- In veel technische literatuur, aangaande (informatie)beveiliging, wordt biometrie beschreven als 'de identificatie en/of authenticatie van een levende individu met behulp van fysieke of gedragskenmerken'

Dreiging:
Een mogelijke gebeurtenis die een ongewenst effect heeft op het beschouwde systeem

Dreigingsagent:
Een persoon, object of toestand die dreigingen veroorzaakt. In het algemeen wordt gekeken naar personen als bron van dreigingen. Deze personen worden ook wel aangeduid als tegenstander. andere algemene bronnen van dreigingen zijn: natuur, buitenwereld, interne systemen

Dreigingsscenario:
Een combinatie van dreiging, tegenstander en IT-middel die samen een incident kunnen doen ontstaan. Het in beschouwing nemen van dreigingsscenario's maakt het mogelijk de gevolgen in kaart te brengen van combinaties van op zichzelf onschuldige gebeurtenissen en ernstige dreigingen die resulteren uit combinaties van minder ernstige dreigingen

Exclusiviteit:
De mate waarin de toegang tot en de kennisname van een informatiesysteem en de informatie daarin is beperkt tot een gedefinieerde groep van gerechtigden

Incident:
Een ongewenste situatie die ontstaat als gevolg van de realisatie van een dreiging; een gebeurtenis waarbij de gewenste eigenschappen van een systeem worden aangetast

Informatiebeveiliging:
Het treffen en onderhouden van een samenhangend pakket van maatregelen ter waarborging van de beschikbaarheid, integriteit en exclusiviteit van een informatiesysteem en daarmee van de informatie daarin

Integriteit:
De mate waarin een informatiesysteem zonder fouten is

Verificatie:
Het proces van vergelijken van het resultaat van een activiteit met de eisen of specificaties behorende bij deze activiteit

10. Afkortingen

AMIDKLu	Afdeling Militaire Inlichtingen Dienst bij de Koninklijke Luchtmacht
AS	Authentication Server
BVD	Binnenlandse Veiligheids Dienst
CPU	Central Processing Unit
DES	Data Encryption Standard
FAR	False Acceptance Rate
FRR	False Rejection Rate
IC	Integrated Circuit
KLu	Koninklijke Luchtmacht
MID	Militaire Inlichtingen Dienst
MITBEP	door TNO opgezette database met informatiebeveiligingsproducten
PIN	Persoonlijk Identificatie Nummer
PC	Personal Computer
PCMCIA	Personal Computer Memory Card International Association
RF	Radio Frequenties
WORM	Write Once Read Many

11. Literatuurlijst

[1] ISO 7816 Identification cards - Integrated circuit(s)cards with contacts - Part 1: Physical characteristics

[2] "Van Dale, Groot woordenboek der Nederlandse taal", van Dale lexicografie, Utrecht, 12de uitgave 1992.

[3] Guinier D., "Identification by biometrics, an introduction and a survey", Sigsac Review, Summer 1990.

[4] Kivits R.W.L.J., "Fundamentele technische keuzen voor een open infrastructuur voor chipkaarttoepassingen en biometrische verificatiesystemen voor zo'n infrastructuur", Afstudeerverslag aan TU Eindhoven, mei 1995

[5] Deane F., Barrelle K., Henderson R. and Mahar D., "Perceived acceptability of biometric security systems", Elsevier Science Ltd., 1995 volume 14.

[6] Veltman M., "Continue biometrische authenticatie op basis van toetsaanslag analyse", Afstudeerverslag Hogeschool Venlo, juni 1996.

[7] "Chipcards en Electronische labels, een verkenning", Ministerië van Economische Zaken, september 1990.

[8] "Advanced authentication technology", Computer systems Laboratory Bulletin, november 1991.

[9] "Guideline for the use of advanced authentication technology alternatives", Federal Information Processing Standards Publication 190, 28 september 1994.

[10] McCurley K.S., "Tokens dumb and smart".

[11] Schneier B., "Smart tokens", 1995.

[12] Miller B.L., "Overview of Biometrics", Conference proceedings Smart Card '95" 14th - 16th february 1995, Londen, UK

[13] "The 1991 Sandia Report, a performance evaluation of biometric identification devices", Recognition Systems, Inc..

[14] "Body Check", Secure Computing, p. 30-39, july 1995.

[15] OSI/IEC DIS 2382-08 Information Technology - Vocabulary - Part 8: Security

12. Ondertekening

D.W. Fikkert	Ing. P.J.A. Verhaar	Ing. T.G.A. van Rhee
Groepsleider	Projectleider/auteur	Auteur

Bijlage A Overzicht producten die gebruikmaken van tokens

Productnaam	Leverancier/ producent	uitvoeringsvorm	Challenge/ Response-mechanisme*	activeringscode voor token of toegangscontro-lesysteem	bruikbaar voor meerdere toe-gangscontrole-systemen
©XS4U®	Infinity	bedrukte kaar-ten van credit-cardformaat	-	-	ja
ActivCard token	ActivCard	calculator	1/4	ja	ja
SecureID	Security Dyna-mics	calculator/ super smart card	3	ja	nee
RB-1 Challenge-Response Token	Cryptocard	super smart card	1	ja	ja
SB-1 Electronic Diskette Token	Cryptocard	Smart disk	1	ja	ja
Watchword II	Racal Datacom	calculator	1	ja	ja
Infocard	Leemah Data-com Security Corporation	super smart card	1	ja	ja
DES-gold	Enigma Logic	super smart card	2	ja	ja
DES-silver	Enigma Logic	super smart card	2	nee	nee

*

1. de challenge is een 'willekeurig' door het toegangscontrolesysteem bepaalde waarde;
2. de challenge is gebaseerd op het aantal keer dat door het toegangscontrolesysteem toegang is verleend aan de betreffende persoon;
3. de challenge is gebaseerd op een, tussen het token en het toegangscontrolesys-teem, gesynchroniseerde klok;
4. de challenge is gebaseerd op een combinatie van een gesynchroniseerde klok en het aantal keer dat toegang is verleend.

Bijlage B Overzicht producten die gebruikmaken van biometrische kenmerken

Biometrisch kenmerk	Productnaam	Leverancier/ producent	Verificatie-tijd [sec.]	Template-grootte [bytes]	Prijs	FAR %	FRR %
Vingerafdruk	TouchSafe II	Indentix Inc.	2	1200	$1395	0,001	1
	FingerCheck	Startek Eng.	2 á 3	256	£1650	0,0001	1
Hand-geometrie	ID3D Handkey	Recognition Systems Inc.	1 á 2	9	$2100	0,8	0,1
Vinger-geometrie	Digi-2	BioMet Partners	1	20	$450	-	-
Retinapatroon	EyeDentifi-cation System 2000	EyeDentify Inc.	1,5	96	$2500	0,000001	1
Irispatroon	IriScan 2000 EAC	IriScan Inc.	2	512	$5950	0,00076-0,00001	0,00076-0,00001
Gezichts-afbeelding	TrueFace	Miros Inc.	1,5	500	$1950	2,5	2,5
Statische handtekening	Chequematch	AEA Technolo-gy	-	-	-	-	-
Dynamische handtekening	Counter-match	AEA Technolo-gy	-	1000	£1000	0,1	0,1
Grondtoon stem	VoiceKey	International Electronics Inc.	6,5	-	$1225	0,9	4,3
	Ver-A-Tel	Alpha Micosys-tem	19,5	-	-	6	6

REPORT DOCUMENTATION PAGE
(MOD-NL)

1. DEFENCE REPORT NO (MOD-NL)	2. RECIPIENT'S ACCESSION NO	3. PERFORMING ORGANIZATION REPORT NO
TD96-0394		FEL-97-A003
4. PROJECT/TASK/WORK UNIT NO	**5. CONTRACT NO**	**6. REPORT DATE**
6025938	A96KLu634	February 1997
7. NUMBER OF PAGES	**8. NUMBER OF REFERENCES**	**9. TYPE OF REPORT AND DATES COVERED**
84 (incl 2 appendices, excl RDP & distribution list)	15	

10. TITLE AND SUBTITLE

Tokens en Biometrie voor Identificatie en Authenticatie
(Tokens and Biometrics for Identification and Authentication)

11. AUTHOR(S)

T.G.A. van Rhee
P.J.A. Verhaar

12. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

TNO Physics and Electronics Laboratory, PO Box 96864, 2509 JG The Hague, The Netherlands
Oude Waalsdorperweg 63, The Hague, The Netherlands

13. SPONSORING AGENCY NAME(S) AND ADDRESS(ES)

Royal Netherlands Airforce
Binckhorstlaan 135, The Hague, The Netherlands

14. SUPPLEMENTARY NOTES

The classification designation Ongerubriceerd is equivalent to Unclassified, Stg. Confidentieel is equivalent to Confidential and Stg. Geheim is equivalent to Secret.

15. ABSTRACT (MAXIMUM 200 WORDS (1044 BYTE))

In the last few years there has been a lot of progression in the development of identification and authentication mechanisms. Tokens are frequently applied within these mechanisms. These tokens can vary from simple magnetic cards to (super)smart cards. (super)Smart cards can operate fully self-employed. Also frequently applied for identification and authentication are biometrics. To obtain a clear insight in the momentary available products and developments TNO-FEL was assigned by the Military Intelligence Service located by the Royal Netherlands Air Force (AMIDKLu) to make a product survey.
The products included in the survey will be tested according to a selected group of threats. This threats are lined up in consultation with the commissioner. This tests will be performed to support possible choices of policy in relation to apply such products.

16. DESCRIPTORS	IDENTIFIERS
Identification	Tokens
Authentication	Threats
Biometrics	Product survey
Smart cards	

17a. SECURITY CLASSIFICATION (OF REPORT)	17b. SECURITY CLASSIFICATION (OF PAGE)	17c. SECURITY CLASSIFICATION (OF ABSTRACT)
Ongerubriceerd	Ongerubriceerd	Ongerubriceerd

18. DISTRIBUTION AVAILABILITY STATEMENT	17d. SECURITY CLASSIFICATION (OF TITLES)
Unlimited Distribution	Ongerubriceerd

Distributielijst

1.	Bureau TNO Defensieonderzoek
2.	Directeur Wetenschappelijk Onderzoek en Ontwikkeling*)
3.	HWO-KL*)
4.	HWO-KLu
5.	HWO-KM*)
6.	HWO-CO*)
7 t/m 9.	KMA, Bibliotheek
10.	AMIDKLu, t.a.v. LtKol P.J.G. Post Uiterweer
11.	AMIDKLu, t.a.v. Drs. ing. F. van Eck
12.	DOPKLu/ACIS, t.a.v. Kol P.O. Arts
13.	DOPKLu/ACIS, t.a.v. Kap E. van Weert
14.	LAS/BO/CIV, t.a.v. Ing. J.P.H.M. Klomp
15.	DEBKM/CABIS, t.a.v. Ing. Th.A.H. Voss
16.	CO/BA
17.	NATCO/OI&T/CCK, t.a.v. A.J. van Gentevoort
18.	Directie TNO-FEL, t.a.v. Dr. J.W. Maas
19.	Directie TNO-FEL, t.a.v. Ir. J.A. Vogel, daarna reserve
20.	Archief TNO-FEL, in bruikleen aan M&P*)
21.	Archief TNO-FEL, in bruikleen aan Dr. ir. J.L.J. de Sonneville
22.	Archief TNO-FEL, in bruikleen aan D.W. Fikkert
23.	Archief TNO-FEL, in bruikleen aan Ir. P.W.M. Franken
24.	Archief TNO-FEL, in bruikleen aan Ir. E. Hardam
25.	Archief TNO-FEL, in bruikleen aan Ing. T.G.A. van Rhee
26.	Archief TNO-FEL, in bruikleen aan Ing. M. Veltman
27.	Archief TNO-FEL, in bruikleen aan Dr. ir. M. Struik
28.	Archief TNO-FEL, in bruikleen aan Ir. H.A.M. Luiijf
29.	Archief TNO-FEL, in bruikleen aan Ing. G.J.M. Peeters
30.	Archief TNO-FEL, in bruikleen aan Ing. P.J.A. Verhaar
31.	Documentatie TNO-FEL
32.	Reserve
	TNO-PML, Bibliotheek**)
	TNO-TM, Bibliotheek**)
	TNO-FEL, Bibliotheek**)

Indien binnen de krijgsmacht extra exemplaren van dit rapport worden gewenst door personen of instanties die niet op de verzendlijst voorkomen, dan dienen deze aangevraagd te worden bij het betreffende Hoofd Wetenschappelijk Onderzoek of, indien het een K-opdracht betreft, bij de Directeur Wetenschappelijk Onderzoek en Ontwikkeling.

*) Beperkt rapport (titelblad, managementuittreksel, RDP en distributielijst).
**) RDP.